NOT YET SCHEDULED FOR ORAL ARGUMENT

Nos. 17-5217, 17-5232

In The United States Court of Appeals
For the District of Columbia Circuit

IN RE: U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION

ON APPEAL FROM THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA (No. 1:15-mc-01394-ABJ)

JOINT APPENDIX

David H. Thompson
Peter A. Patterson
COOPER & KIRK, PLLC
1523 New Hampshire Avenue, N.W.
Washington, D.C. 20036

Tina Wolfson
AHDOOT & WOLFSON, PC
1016 Palm Avenue
West Hollywood, CA 90069

John Yanchunis
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 North Franklin Street, 7th Floor
Tampa, FL 33602

Plaintiffs' Steering Committee

GIRARD GIBBS LLP
Daniel C. Girard
Jordan Elias
601 California Street, 14th Floor
San Francisco, CA 94108
Phone: (415) 981-4800
Facsimile: (415) 981-4846
Email: dcg@girardgibbs.com

Interim Lead Class Counsel

Gary E. Mason
WHITFIELD BRYSON & MASON LLP
5101 Wisconsin Avenue, N.W.
Washington, D.C. 20016

Liaison Counsel

Additional Counsel listed on inside cover

Gregory O'Duden
Larry Adkins
Paras N. Shah
Allison C. Giles
NATIONAL TREASURY EMPLOYEES UNION
1750 H Street, N.W.
Washington, D.C. 20006
Phone: (202) 572-5500
Email: greg.oduden@nteu.org
Email: larry.adkins@nteu.org
Email: paras.shah@nteu.org
Email: allie.giles@nteu.org

Counsel for Appellants National Treasury Employees Union, Eugene Gambardella, Stephen Howell, and Jonathon Ortino

Sonia M. Carson
Mark B. Stern
U.S. DEPARTMENT OF JUSTICE
Civil Division, Appellate Staff
950 Pennsylvania Avenue, N.W.
Room 7234
Washington, D.C. 20530

Counsel for Defendants-Appellees U.S. Office of Personnel Management, Director Jeff T.H. Pon, Chief Information Officer David Garcia, and the U.S. Department of Homeland Security

F. Joseph Warin
Jason J. Mendro
Matthew S. Rozen
Jeremy M. Christiansen
GIBSON, DUNN & CRUTCHER LLP
1050 Connecticut Avenue, N.W.
Washington, D.C. 20036
Phone: (202) 955-8500
Fax: (202) 530-9575
Email: fwarin@gibsondunn.com
jmendro@gibsondunn.com
mrozen@gibsondunn.com
jchristiansen@gibsondunn.com

Counsel for Defendant-Appellee KeyPoint Government Solutions, Inc.

JOINT APPENDIX TABLE OF CONTENTS

APPEAL,CLOSED,JURY,MDL,TYPE I−PRIVACY

U.S. District Court
District of Columbia (Washington, DC)
CIVIL DOCKET FOR CASE #: 1:15−mc−01394−ABJ

IN RE: U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION
Assigned to: Judge Amy Berman Jackson
Cases: 1:15−cv−01015−ABJ
1:15−cv−01321−ABJ
1:15−cv−01449−ABJ
1:15−cv−01564−ABJ
1:15−cv−01617−ABJ
1:15−cv−01653−ABJ
1:15−cv−01933−ABJ
1:15−cv−02089−ABJ
1:15−cv−02259−ABJ
1:15−cv−01808−ABJ
1:16−cv−00178−ABJ
1:15−cv−01752−ABJ
1:16−cv−00392−ABJ
1:16−cv−01253−ABJ
1:15−cv−01927−ABJ
1:15−cv−01928−ABJ
1:15−cv−01929−ABJ
1:15−cv−01930−ABJ
1:15−cv−01931−ABJ
1:15−cv−01810−ABJ
1:15−cv−01835−ABJ
Case in other court: USCA, 17−05217
USCA, 17−05232
Federal Circuit, 18−01182−CB
Judicial Panel on Multidistrict Litigation, 2664
Cause: 05:552 Freedom of Information Act

Date Filed: 10/09/2015
Date Terminated: 09/20/2017
Jury Demand: Plaintiff
Nature of Suit: 890 Other Statutory Actions
Jurisdiction: U.S. Government Defendant

In Re

IN RE: U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION

Plaintiff

AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL−CIO

represented by **Daniel C. Girard**
GIRARD GIBBS LLP
601 California Street
14th Floor
San Francisco, CA 94108
(415) 981−4800
Fax: (415) 981−4846
Email: dcg@girardgibbs.com
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Gary Edward Mason
WHITFIELD BRYSON & MASON LLP
5101 Wisconsin Avenue, NW

Suite 305
Washington, DC 20016
(202) 429−2290
Fax: (202) 429−2294
Email: gmason@wbmllp.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Jordan Elias
GIRARD GIBBS LLP
601 California Street
14th Floor
San Francisco, CA 94108
(415) 981−4800
Fax: (415) 981−4846
Email: je@girardgibbs.com
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

ROBERT CRAWFORD represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Gary Edward Mason
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Jordan Elias
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Adam E. Polk
GIRARD GIBBS LLP
601 California Street
14th Floor
San Francisco, CA 94108
(415) 544−6280
Fax: (415) 981−4846
Email: aep@girardgibbs.com
PRO HAC VICE
ATTORNEY TO BE NOTICED

Christopher K. Hikida
GIRARD GIBBS LLP
601 California Street
14th Floor
San Francisco, CA 94108
(415) 981−4800
Fax: (415) 981−4846
Email: ckh@girardgibbs.com
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

ADAM DALE represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY

PRO HAC VICE
ATTORNEY TO BE NOTICED

Gary Edward Mason
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Jordan Elias
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Adam E. Polk
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Christopher K. Hikida
(See above for address)
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

NATIONAL TREASURY EMPLOYEES UNION

represented by **Paras N. Shah**
NATIONAL TREASURY EMPLOYEES UNION
Office of General Counsel
1750 H Street, NW
Washington, DC 20006
(202) 572−5553
Fax: (202) 572−5645
Email: paras.shah@nteu.org
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Plaintiff

STEPHEN HOWELL

represented by **Paras N. Shah**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Plaintiff

JOHN ORTINO

represented by **Paras N. Shah**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Plaintiff

MARY C. WOO
on behalf of herself and all others similarly situated

represented by **Anna C. Haac**
TYCKO & ZAVAREEI, LLP
1828 L Street, NW
Suite 1000
Washington, DC 20036
(202) 973−0900
Fax: (202) 973−0950
Email: ahaac@tzlegal.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Hassan A. Zavareei

TYCKO & ZAVAREEI, LLP
1828 L Street, NW
Suite 1000
Washington, DC 20036
(202) 973−0900
Fax: (202) 973−0950
Email: hzavareei@tzlegal.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Norman E. Siegel
STUEVE SIEGEL HANSON LLP
460 Nichols Road
Suite 200
Kansas City, MO 64112
(816) 714−7100
Fax: (816) 714−7101
Email: siegel@stuevesiegel.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Plaintiff

TERESA J. MCGARRY
The Honorable, on behalf of herself and all others similarly situated

represented by

Daniel C. Girard
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Denis F. Sheils
KOHN, SWIFT & GRAF, P.C.
One South Broad Street
Suite 2100
Philadelphia, PA 19107
(215) 238−1700
Fax: (215) 238−1968
Email: dsheils@kohnswift.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Plaintiff

VICTOR W. HOBBS
on behalf of himself and all others similarly situated

represented by

Behram Parekh
KIRTLAND & PACKARD LLP
2041 Rosecrans Avenue
Suite 300
El Segundo, CA 90245
(310) 536−1000
Fax: (310) 536−1001
Email: bvp@kirtlandpackard.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Plaintiff

HECTOR PEREZ
individually, and on behalf of all others similarly situated

represented by

Frazer Walton , Jr.
LAW OFFICE OF FRAZER WALTON, JR.
1913 D Street, NE
Washington, DC 20002
(202) 398−8920
Email: frawalton@verizon.net
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

John Yanchunis

MORGAN & MORGAN COMPLEX
LITIGATION GROUP
201 N. Franklin Street
7th Floor
Tampa, FL 33602
(813) 275−5272
Fax: (813) 275−9295
Email: jyanchunis@forthepeople.com
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Marcio W. Valladares
MORGAN & MORGAN COMPLEX
LITIGATION GROUP
201 N. Franklin Street
7th Floor
Tampa, FL 33602
(813) 229−4044
Fax: (813) 222−4733
Email: mvalladares@forthepeople.com
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Patrick A. Barthle , II
MORGAN & MORGAN COMPLEX
LITIGATION GROUP
201 N. Franklin Street
7th Floor
Tampa, FL 33602
(813) 223−5505
Fax: (813) 222−4738
Email: pbarthle@forthepeople.com
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Steven William Teppler
ABBOTT LAW GROUP P.A.
2929 Plummer Cove Road
Jacksonville, FL 32223
Email: steppler@abbottlawpa.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Plaintiff

JOHN ORAVIS
individually, and on behlaf of all others similarly situated

represented by **Frazer Walton , Jr.**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Steven William Teppler
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Plaintiff

GARY S. COX
individually and on behalf of all others similarly situated

represented by **Carin L. Marcussen**
FEDERMAN & SHERWOOD
10205 N. Pennsylvania Avenue
Oklahoma City, OK 73120
(405) 235−1560
Fax: (405) 239−2112

Email: clm@federmanlaw.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Plaintiff

DERRICK SIMS
individually, and on behalf of all others similarly situated

Plaintiff

MICHAEL HANAGAN
individually and on behalf of all others similarly situated

represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Graham B. LippSmith
KASDAN LIPPSMITH WEBER TURNER LLP
500 S. Grand Avenue
Suite 1310
Los Angeles, CA 90071
(213) 254−4800
Fax: (213) 254−4801
Email: glippsmith@klwtlaw.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Plaintiff

EDWARD W. KRIPPENDORF
on behalf of himself and all others similarly situated

represented by **Corban S. Rhodes**
LABATON SUCHAROW LLP
140 Broadway
New York, NY 10005
(212) 907−0761
Fax: (212) 818−0477
Email: crhodes@labaton.com
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Garrett J. Bradley
LABATON SUCHAROW LLP
140 Broadway
New York, NY 10005
(212) 907−0735
Fax: (212) 818−0477
Email: gbradley@labaton.com
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

J. Jonathan Schraub
SANDS ANDERSON PC
1497 Chain Bridge Road
Suite 202
McLean, VA 22101
(703) 893−3600
Fax: (703) 893−8484
Email: jjschraub@sandsanderson.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joel H. Bernstein

LABATON SUCHAROW LLP
140 Broadway
New York, NY 10005
(212) 907−0869
Fax: (212) 883−7069
Email: jbernstein@labaton.com
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

EDWARD L. ROBBELOTH
on behalf of themselves and all others similarly situated

represented by **Corban S. Rhodes**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Garrett J. Bradley
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

J. Jonathan Schraub
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joel H. Bernstein
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

ERIC W. EDGAR
on behalf of themselves and all others similarly situated

represented by **Corban S. Rhodes**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Garrett J. Bradley
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

J. Jonathan Schraub
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joel H. Bernstein
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

JOHN RABER
on behalf of themselves and all others similarly situated

represented by **Corban S. Rhodes**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE

ATTORNEY TO BE NOTICED

Garrett J. Bradley
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

J. Jonathan Schraub
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joel H. Bernstein
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

MICAELA BROWN
On Behalf of Herself and all Others Similarly Situated

represented by **Charles J. LaDuca**
CUNEO GILBERT & LADUCA, LLP
4725 Wisconsin Avenue, NW
Suite 200
Washington, DC 20016
(202) 789−3960
Fax: (202) 789−1813
Email: charles@cuneolaw.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Monica E. Miller
CUNEO GILBERT & LADUCA, LLP
4725 Wisconsin Avenue, NW
Suite 200
Washington, DC 20016
(202) 789−3960
Fax: (202) 789−1813
Email: monica@cuneolaw.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Plaintiff

RYAN BONNER
On Behalf of Himself and all Others Similarly Situated

represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

David Henry Thompson
COOPER & KIRK, PLLC
1523 New Hampshire Ave, NW
Washington, DC 20036
(202) 220−9600
Fax: (202) 220−9601
Email: dthompson@cooperkirk.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Peter A. Patterson
COOPER & KIRK, PLLC
1523 New Hampshire Ave, NW
Washington, DC 20036
(202) 220−9600

Fax: (202) 220−9601
Email: ppatterson@cooperkirk.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Plaintiff

NICOLE WAID
on behalf of herself and all others similarly situated

represented by **Corban S. Rhodes**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Garrett J. Bradley
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

J. Jonathan Schraub
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joel H. Bernstein
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

NICHOLAS D. CAVIS
on behalf of themselves and all others similarly situated

represented by **J. Jonathan Schraub**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joel H. Bernstein
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Plaintiff

WILLIAM PRESTON
on behalf of themselves and all others similarly situated

represented by **J. Jonathan Schraub**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joel H. Bernstein
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Plaintiff

HOWARD SMITH
individually and on behalf of all others similarly situated

represented by **Patrick A. Malone**
PATRICK MALONE & ASSOCIATES, P.C.
1310 L Street, NW
Suite 800
Washington, DC 20005
(202) 742−1500
Fax: (202) 742−1515
Email: pmalone@patrickmalonelaw.com
LEAD ATTORNEY

ATTORNEY TO BE NOTICED

Tina Wolfson
AHDOOT & WOLFSON, PC
10728 Lindbrook Drive
Los Angeles, CA 90024
(310) 474−9111
Fax: (310) 474−8585
Email: twolfson@ahdootwolfson.com
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

CHAD KAPPERS represented by **Mark Robert Rosen**
BARRACK, RODOS & BACINE
3300 Two Commerce Square
2001 Market Street
Philadelphia, PA 19103
(215) 963−0600
Fax: (215) 963−0838
Email: mrosen@barrack.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Plaintiff

WILLIAM FLEISHELL III represented by **Mark Robert Rosen**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Plaintiff

JERAN BINNING
on Behalf of Himself and All Others Similarly Situated represented by **Robert K. Shelquist**
LOCKRIDGE GRINDAL NAUEN P.L.L.P.
100 Washington Avenue South
Suite 2200
Minneapolis, MN 55401
(612) 339−6900
Fax: (612) 339−0981
Email: rkshelquist@locklaw.com
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

ADEDEJI SHAMONDA represented by **ADEDEJI SHAMONDA**
P.O. Box 881773
San Francisco, CA 94188−1773
415−531−8844
PRO SE

Plaintiff

ADEBIYI K. SHAMONDA represented by **ADEBIYI K. SHAMONDA**
3120 Shelter Creek Lane
San Bruno, CA 94066
(415) 812−4243
PRO SE

Plaintiff

MARIO SAMPEDRO represented by

Daniel C. Girard
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

GARDELL BRANCH represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

ROBERT SLATER represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

JANE DOE II represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

TORALF PETERS represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

MYRNA BROWN represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

CHARLENE OLIVER represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

DARREN STRICKLAND represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

CYNTHIA KING−MYERS represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE

ATTORNEY TO BE NOTICED

Plaintiff

TRAVIS ARNOLD represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

MICHAEL JOHNSON represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

TONY BACHTELL represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

ZACHARY SHARPER represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

JENNIFER GUM represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

JOHN DOE III represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

JOHN DOE II represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

JOHN DOE represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

MICHAEL EBERT represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

DEBORAH HOFFMAN represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

PAUL DALY represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

LILLIAN GONZALEZ−COLON represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

KELLY FLYNN represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

PETER ULIANO represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

RYAN LOZAR represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

ORIN GRIFFITH represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

TIMOTHY SEBERT represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE

ATTORNEY TO BE NOTICED

Plaintiff

JOHNNY GONZALEZ represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

MARYANN HIBBS represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

ALIA FULI represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

HEATHER BURNETT−RICK represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

MONTY BOS represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

JANE DOE represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

NANCY WHEATLEY represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

KIMBERLY WINSOR represented by **Daniel C. Girard**
(See above for address)
LEAD ATTORNEY
PRO HAC VICE
ATTORNEY TO BE NOTICED

Plaintiff

EUGENE GAMBARDELLA represented by **Paras N. Shah**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Plaintiff

DAVID A. GOLDEN
individually, and as parent and next friend of Connor B. Golden, a minor

represented by **Eric J. Artrip**
MASTANDO & ARTRIP, LLC
301 Washington Street
Suite 302
Huntsville, AL 35801
(256) 532−2222
Fax: (256) 513−7489
Email: artrip@mastandoartrip.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Plaintiff

RONNIE GOLDEN
on behalf of themselves and all others similarly situated

represented by **Eric J. Artrip**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Plaintiff

LILIANA GOLDEN
on behalf of themselves and all others similarly situated

represented by **Eric J. Artrip**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

V.

Defendant

UNITED STATES OFFICE OF PERSONNEL MANAGEMENT
Beth F. Cobert, acting Director, in her official capacity; Donna Seymour, Chief Information Officer, in her official capacity

represented by **Andrew Evan Carmichael**
U.S. DEPARTMENT OF JUSTICE
Ben Franklin Station
P.O. Box 883
Washington, DC 20044
(202) 514−3346
Fax: (202) 616−8460
Email: andrew.e.carmichael@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Elizabeth J. Shapiro
U.S. DEPARTMENT OF JUSTICE
Civil Division, Federal Programs Branch
P.O. Box 883
Washington, DC 20530
(202) 514−5302
Fax: (202) 616−8202
Email: Elizabeth.Shapiro@usdoj.gov
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Evan Borson
U.S. DEPARTMENT OF JUSTICE
Civil Division, Federal Programs Branch
20 Massachusetts Avenue NW
Washington, DC 20530
(202) 514−1944
Fax: (202) 616−8460
Email: joseph.borson@usdoj.gov

LEAD ATTORNEY
ATTORNEY TO BE NOTICED

John Kenneth Theis
U.S. DEPARTMENT OF JUSTICE
P.O. Box 883
Washington, DC 20044
(202) 305−7632
Fax: (202) 616−8460
Email: john.k.theis@usdoj.gov
TERMINATED: 04/26/2016

Kieran Gavin Gostin
U.S. DEPARTMENT OF JUSTICE
Civil Division, Federal Programs Branch
P.O. Box 883
Washington, DC 20044
(202) 353−4556
Fax: (202) 616−8460
Email: kieran.g.gostin@usdoj.gov
TERMINATED: 10/28/2016

Matthew A. Josephson
U.S. DEPARTMENT OF JUSTICE
Civil Division, Federal Programs Branch
P.O. Box 883
Washington, DC 20044
(202) 514−9237
Fax: (202) 616−8470
Email: Matthew.A.Josephson@usdoj.gov
TERMINATED: 12/15/2016

Paul G. Freeborne
U.S. DEPARTMENT OF JUSTICE
Civil Division, Federal Programs Branch
P.O. Box 883
Washington, DC 20001
(202) 353−0543
Fax: (202) 616−8470
Email: paul.freeborne@usdoj.gov
TERMINATED: 03/03/2016

Defendant

DONNA SEYMOUR
Chief Information Officer of U.S. Office of Personnel Management, in her official capacity

represented by **Andrew Evan Carmichael**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Elizabeth J. Shapiro
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Evan Borson
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

John Kenneth Theis
(See above for address)
TERMINATED: 04/26/2016

Kieran Gavin Gostin
(See above for address)

TERMINATED: 10/28/2016

Matthew A. Josephson
(See above for address)
TERMINATED: 12/15/2016

Paul G. Freeborne
(See above for address)
TERMINATED: 03/03/2016

Defendant

KEYPOINT GOVERNMENT SOLUTIONS
a Delaware corporation

represented by

Alexander H. Southwell
GIBSON, DUNN & CRUTCHER, L.L.P.
200 Park Avenue
48th Floor
New York, NY 10166−0193
(212) 351−3981
Fax: (212) 351−6281
Email: asouthwell@gibsondunn.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Francis Joseph Warin
GIBSON, DUNN & CRUTCHER, LLP
1050 Connecticut Avenue, NW
Washington, DC 20036
(202) 887−3609
Fax: (202) 530−9608
Email: fwarin@gibsondunn.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Jason J. Mendro
GIBSON, DUNN & CRUTCHER, LLP
1050 Connecticut Avenue, NW
Suite 200
Washington, DC 20036
(202) 887−3726
Fax: (202) 530−9626
Email: jmendro@gibsondunn.com
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Defendant

BETH F. COBERT
Acting Director of United States Office of Personnel Management, in her Official Capacity

represented by

Andrew Evan Carmichael
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Elizabeth J. Shapiro
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Evan Borson
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

John Kenneth Theis
(See above for address)
TERMINATED: 04/26/2016

Kieran Gavin Gostin

(See above for address)
TERMINATED: 10/28/2016

Matthew A. Josephson
(See above for address)
TERMINATED: 12/15/2016

Paul G. Freeborne
(See above for address)
TERMINATED: 03/03/2016

Defendant

KATHERINE ARCHULETA
former Director of U.S. Office of Personnel Management, in her official capacity

represented by **Andrew Evan Carmichael**
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

Joseph Evan Borson
(See above for address)
LEAD ATTORNEY
ATTORNEY TO BE NOTICED

John Kenneth Theis
(See above for address)
TERMINATED: 04/26/2016

Kieran Gavin Gostin
(See above for address)
TERMINATED: 10/28/2016

Matthew A. Josephson
(See above for address)
TERMINATED: 12/15/2016

Defendant

UNITED STATES DEPARTMENT OF HOMELAND SECURITY

represented by **John Kenneth Theis**
(See above for address)
TERMINATED: 04/26/2016

Kieran Gavin Gostin
(See above for address)
TERMINATED: 10/28/2016

Defendant

ELAINE D. KAPLAN

represented by **ELAINE D. KAPLAN**
PRO SE

Kieran Gavin Gostin
(See above for address)
TERMINATED: 10/28/2016

Matthew A. Josephson
(See above for address)
TERMINATED: 12/15/2016

Defendant

JOHN BERRY

represented by **JOHN BERRY**
PRO SE

Kieran Gavin Gostin
(See above for address)
TERMINATED: 10/28/2016

Matthew A. Josephson
(See above for address)
TERMINATED: 12/15/2016

Defendant

DOES
1 through 100 inclusive

Date Filed	#	Docket Text
10/09/2015	1	COPY OF TRANSFER ORDER dated 10/9/2015 from the Judicial Panel on Multidistrict Litigation directing the transfer to the U.S. District Court for the District of Columbia, with the consent of that court, assigned to the Honorable Judge Amy Berman Jackson for coordinated pretrial proceedings pursuant to 28 U.S.C. 1407.(MDL 2664) (ztnr) (Entered: 10/16/2015)
10/27/2015	5	COPY OF CONDITIONAL TRANSFER ORDER (CTO−1) dated 10/27/15 from the Judicial Panel on Multidistrict Litigation directing the transfer to the U.S. District Court for the District of Columbia with the consent of that court, assigned to the Honorable Judge Amy Berman Jackson for coordinated pretrial proceedings pursuant to 28 U.S.C. 1407.(MDL 2664) (ztnr) (Entered: 10/29/2015)
10/29/2015	2	NOTICE of Appearance by Paras N. Shah on behalf of STEPHEN HOWELL, NATIONAL TREASURY EMPLOYEES UNION, JOHN ORTINO (Shah, Paras) (Entered: 10/29/2015)
10/29/2015	3	NOTICE of Appearance by Gregory J. O'Duden on behalf of STEPHEN HOWELL, NATIONAL TREASURY EMPLOYEES UNION, JOHN ORTINO (O'Duden, Gregory) (Entered: 10/29/2015)
10/29/2015	4	NOTICE of Appearance by Larry J. Adkins on behalf of STEPHEN HOWELL, NATIONAL TREASURY EMPLOYEES UNION, JOHN ORTINO (Adkins, Larry) (Entered: 10/29/2015)
11/02/2015	6	NOTICE of Appearance by Devki Kaur Virk on behalf of STEPHEN HOWELL, NATIONAL TREASURY EMPLOYEES UNION, JOHN ORTINO (Virk, Devki) (Entered: 11/02/2015)
11/02/2015	7	NOTICE of Appearance by Leon Dayan on behalf of STEPHEN HOWELL, NATIONAL TREASURY EMPLOYEES UNION, JOHN ORTINO (Dayan, Leon) (Entered: 11/02/2015)
11/10/2015	8	INITIAL PRACTICE AND PROCEDURE ORDER. See Order for details. Signed by Judge Amy Berman Jackson on 11/10/15. (DMK) (Entered: 11/10/2015)
11/13/2015	9	NOTICE of Appearance by Behram Parekh on behalf of VICTOR W. HOBBS (Parekh, Behram) (Entered: 11/13/2015)
11/16/2015	10	NOTICE of Appearance by Graham B. LippSmith on behalf of MICHAEL HANAGAN (LippSmith, Graham) (Entered: 11/16/2015)
11/16/2015	11	NOTICE of Appearance by Norman E. Siegel on behalf of MARY C. WOO (Siegel, Norman) (Entered: 11/16/2015)
11/18/2015	12	NOTICE of Appearance by Daniel C. Girard on behalf of AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL−CIO (Girard, Daniel) (Entered: 11/18/2015)
11/19/2015	13	NOTICE of Appearance by David Henry Thompson on behalf of RYAN BONNER (Thompson, David) (Entered: 11/19/2015)
12/07/2015	14	NOTICE of Appearance by Denis F. Sheils on behalf of TERESA J. MCGARRY (Sheils, Denis) (Entered: 12/07/2015)
12/08/2015	15	Joint STATUS REPORT by KATHERINE ARCHULETA, JOHN BERRY, BETH F. COBERT, ELAINE D. KAPLAN, KEYPOINT GOVERNMENT SOLUTIONS,

		DONNA SEYMOUR, UNITED STATES DEPARTMENT OF HOMELAND SECURITY, UNITED STATES OFFICE OF PERSONNEL MANAGEMENT. (Theis, John) (Entered: 12/08/2015)
12/10/2015	16	NOTICE of Appearance by Carin L. Marcussen on behalf of GARY S. COX (Marcussen, Carin) (Entered: 12/10/2015)
12/14/2015		Set/Reset Hearings: The Initial Scheduling and Case Management Conference is scheduled for Tuesday, December 15, 2015, at 10:00 AM in Courtroom 3 before Judge Amy Berman Jackson. (jth) (Entered: 12/14/2015)
12/14/2015	17	NOTICE *of Withdrawal of Daniel Reilly For Consideration as Liaison Counsel* by AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL−CIO, RYAN BONNER, MICAELA BROWN, NICHOLAS D. CAVIS, GARY S. COX, ROBERT CRAWFORD, ADAM DALE, ERIC W. EDGAR, MICHAEL HANAGAN, VICTOR W. HOBBS, STEPHEN HOWELL, EDWARD W. KRIPPENDORF, TERESA J. MCGARRY, NATIONAL TREASURY EMPLOYEES UNION, JOHN ORAVIS, JOHN ORTINO, HECTOR PEREZ, WILLIAM PRESTON, JOHN RABER, EDWARD L. ROBBELOTH, NICOLE WAID, MARY C. WOO (Mason, Gary) (Entered: 12/14/2015)
12/15/2015		Minute Entry for proceedings held before Judge Amy Berman Jackson: Initial Scheduling and Case Management Conference held on 12/15/2015. (Scheduling Order to be Issued) (Court Reporter: Janice Dickman) (jth) (Entered: 12/15/2015)
12/15/2015	18	NOTICE of Appearance by Alexander H. Southwell on behalf of KEYPOINT GOVERNMENT SOLUTIONS (Southwell, Alexander) (Entered: 12/15/2015)
12/15/2015	19	ORDER setting schedule for further proceedings. It is ORDERED that motions for appointment as plaintiffs' Liaison or Interim Lead Class Counsel are due December 22, 2015; plaintiffs' responses are due January 5, 2016; defendants' responses are due January 12, 2016; and a hearing on the motions is set for January 21, 2016 at 10:00 a.m. in Courtroom 3. It is further ORDERED that a consolidated amended complaint shall be filed approximately 30 days after appointment of Interim Lead Class Counsel. It is further ORDERED that motions to dismiss will be due approximately 60 days after the filing of the CAC, oppositions will be due approximately 45 days after that, and replies will be due approximately 21 days thereafter. Finally, it is ORDERED that discovery is stayed pending resolution of the motions to dismiss. SEE ORDER FOR DETAILS. Signed by Judge Amy Berman Jackson on 12/15/15. (DMK) (Entered: 12/15/2015)
12/16/2015		Set/Reset Deadlines/Hearings: Motions for Appointment as Plaintiffs' Liaison or Interim Lead Class Counsel are due 12/22/2015; Plaintiffs' Responses are due 1/5/2016; Defendants' Responses are due 1/12/2016; A Hearing on the Motions is set for 1/21/2016 at 10:00 AM in Courtroom 3 before Judge Amy Berman Jackson. (jth) (Entered: 12/16/2015)
12/17/2015	20	NOTICE OF RELATED CASE by KEYPOINT GOVERNMENT SOLUTIONS. Case related to Case No. 15−cv−2686 (S.D. Cal.). (Attachments: # 1 Exhibit)(Mendro, Jason) (Entered: 12/17/2015)
12/17/2015	21	TRANSCRIPT OF PROCEEDINGS before Judge Amy Berman Jackson held on December 15, 2015; Page Numbers: 1−60. Date of Issuance: December 17, 2015. Court Reporter/Transcriber Janice Dickman, Telephone number 202−354−3267, Transcripts may be ordered by submitting the Transcript Order Form.<P></P><P></P>For the first 90 days after this filing date, the transcript may be viewed at the courthouse at a public terminal or purchased from the court reporter referenced above. After 90 days, the transcript may be accessed via PACER. Other transcript formats, (multi−page, condensed, CD or ASCII) may be purchased from the court reporter.<P>**NOTICE RE REDACTION OF TRANSCRIPTS:** The parties have twenty−one days to file with the court and the court reporter any request to redact personal identifiers from this transcript. If no such requests are filed, the transcript will be made available to the public via PACER without redaction after 90 days. The policy, which includes the five personal identifiers specifically covered, is located on our website at www.dcd.uscourts.gov.<P></P> Redaction Request due 1/7/2016. Redacted Transcript Deadline set for 1/17/2016. Release of Transcript

		Restriction set for 3/16/2016.(Dickman, Janice) (Entered: 12/17/2015)
12/18/2015	22	NOTICE of Change of Address by Hassan A. Zavareei (Zavareei, Hassan) (Entered: 12/18/2015)
12/21/2015		MINUTE ORDER clarifying Order of December 15, 2015. It is ORDERED that motions for appointment as plaintiffs' Liaison or Interim Lead Class may be filed in the form of an application instead of a motion. It is further ORDERED that applications for membership on the plaintiffs' steering committee are also due by December 22, 2015 and shall follow the schedule set forth in the December 15, 2015 Order: applications are due by December 22, 2015; plaintiffs' responses, if any, are due by January 5, 2016; defendants' responses, if any, are due by January 12, 2016; and a hearing on the applications will be held on January 21, 2016 at 10:00 a.m. in Courtroom 3. Any attorney who has submitted an application seeking membership only to the steering committee, but not as Liaison or Interim Lead Counsel, may attend the hearing by telephone. Signed by Judge Amy Berman Jackson on 12/21/15. (DMK) (Entered: 12/21/2015)
12/22/2015	23	NOTICE *Application of Gary E. Mason for Appointment as Liaison Counsel* by AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL−CIO, RYAN BONNER, MICAELA BROWN, NICHOLAS D. CAVIS, GARY S. COX, ROBERT CRAWFORD, ADAM DALE, ERIC W. EDGAR, MICHAEL HANAGAN, VICTOR W. HOBBS, STEPHEN HOWELL, EDWARD W. KRIPPENDORF, TERESA J. MCGARRY, NATIONAL TREASURY EMPLOYEES UNION, JOHN ORAVIS, JOHN ORTINO, HECTOR PEREZ, WILLIAM PRESTON, JOHN RABER, EDWARD L. ROBBELOTH, DERRICK SIMS, HOWARD SMITH, NICOLE WAID, MARY C. WOO (Attachments: # 1 Certificate of Service, # 2 Exhibit A, # 3 Exhibit B)(Mason, Gary) (Entered: 12/22/2015)
12/22/2015	24	NOTICE *Application of Kohn Swift & Graf, P.C. to be Appointed to the Plaintiffs' Steering Committee, along with the Declaration of Denis F. Sheils* by TERESA J. MCGARRY (Attachments: # 1 Certificate of Service)(Sheils, Denis) (Entered: 12/22/2015)
12/22/2015	25	NOTICE *Application of Norman E. Siegel for Appointment as Interim Lead Class Counsel and Hassan Zavareei for Appointment as Liaison Counsel* by MARY C. WOO (Attachments: # 1 Certificate of Service, # 2 Exhibit A, # 3 Exhibit B)(Siegel, Norman) (Entered: 12/22/2015)
12/22/2015	26	MOTION to Appoint Counsel *(Mark Rosen) to Serve on Plaintiffs' Steering Committee* by CHAD KAPPERS, WILLIAM FLEISHELL III (Rosen, Mark) (Entered: 12/22/2015)
12/22/2015	27	MEMORANDUM re 26 MOTION to Appoint Counsel *(Mark Rosen) to Serve on Plaintiffs' Steering Committee* filed by WILLIAM FLEISHELL III, CHAD KAPPERS by WILLIAM FLEISHELL III, CHAD KAPPERS. (Attachments: # 1 Exhibit A − Firm Biography)(Rosen, Mark) (Entered: 12/22/2015)
12/22/2015	28	NOTICE of Proposed Order by WILLIAM FLEISHELL III, CHAD KAPPERS re 27 Memorandum, 26 MOTION to Appoint Counsel *(Mark Rosen) to Serve on Plaintiffs' Steering Committee* (Rosen, Mark) (Entered: 12/22/2015)
12/22/2015	29	NOTICE *APPLICATION OF BEHRAM V. PAREKH TO PLAINTIFFS' STEERING COMMITTEE* by VICTOR W. HOBBS (Attachments: # 1 Declaration Behram V. Parekh, # 2 Exhibit A, # 3 Exhibit B, # 4 Certificate of Service)(Parekh, Behram) (Entered: 12/22/2015)
12/22/2015	30	CERTIFICATE OF SERVICE by WILLIAM FLEISHELL III, CHAD KAPPERS re 27 Memorandum, 26 MOTION to Appoint Counsel *(Mark Rosen) to Serve on Plaintiffs' Steering Committee*, 28 Notice of Proposed Order . (Rosen, Mark) (Entered: 12/22/2015)
12/22/2015	31	APPLICATION to Appoint Counsel *John Yanchunis as Lead Class Counsel or Co−Lead Class Counsel* by HECTOR PEREZ (Attachments: # 1 Exhibit John A. Yanchunis Resume) (Valladares, Marcio) (Entered: 12/22/2015)
12/22/2015	32	NOTICE *Application for Appointment of Federman & Sherwood to Plaintiffs' Steering Committee and Brief in Support* by GARY S. COX re 19 Order,,, (Attachments: # 1

		Exhibit 1, # 2 Exhibit 2, # 3 Exhibit 3, # 4 Exhibit 4, # 5 Exhibit 5)(Federman, William) (Entered: 12/22/2015)
12/22/2015	33	APPLICATION to Appoint Counsel *Labaton Sucharow LLP and Labaton partner Joel H. Bernstein as Interim Lead Counsel and Sands Anderson, P.C. and Sands partner J. Jonathan Schraub as Liaison Counsel* by NICHOLAS D. CAVIS, ERIC W. EDGAR, EDWARD W. KRIPPENDORF, WILLIAM PRESTON, JOHN RABER, EDWARD L. ROBBELOTH, NICOLE WAID (Attachments: # 1 Declaration of Joel H. Bernstein, # 2 Declaration of J. Jonathan Schraub, # 3 Declaration of Nicole Waid, # 4 Declaration of Edward L. Robbeloth, # 5 Declaration of Eric W. Edgar, # 6 Declaration of William Preston, # 7 Declaration of Nicholas D. Cavis, # 8 Declaration of Edward W. Krippendorf, # 9 Declaration of John Raber)(Bernstein, Joel) (Entered: 12/22/2015)
12/22/2015	34	NOTICE *Application for Appointment of Girard Gibbs LLP as Interim Lead Class Counsel* by AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL−CIO, ROBERT CRAWFORD, ADAM DALE (Attachments: # 1 Declaration of Daniel C. Girard, # 2 Exhibit A, # 3 Exhibit B, # 4 Certificate of Service)(Girard, Daniel) (Entered: 12/22/2015)
12/22/2015	35	NOTICE *of Application for Appointment of Cooper & Kirk, PLLC and Kessler Topaz Meltzer & Check, LLP as Interim Co−Lead Class Counsel* by RYAN BONNER (Attachments: # 1 Text of Proposed Order)(Thompson, David) (Entered: 12/22/2015)
12/22/2015	36	MEMORANDUM by RYAN BONNER. (Attachments: # 1 Exhibit 1, # 2 Exhibit 2, # 3 Exhibit 3, # 4 Exhibit 4, # 5 Exhibit 5)(Thompson, David) (Entered: 12/22/2015)
12/22/2015	37	NOTICE *of Application of Tina Wolfson of Ahdoot & Wolfson, PC for Appointment to Plaintiffs Steering Committee* by HOWARD SMITH (Attachments: # 1 Certificate of Service, # 2 Exhibit A)(Wolfson, Tina) (Entered: 12/22/2015)
12/22/2015	38	NOTICE *of Application of Charles J. LaDuca to Plaintiffs' Steering Committee* by MICAELA BROWN (Attachments: # 1 Exhibit Exh. A − CGL Resume, # 2 Certificate of Service)(LaDuca, Charles) (Entered: 12/22/2015)
12/22/2015	39	NOTICE *of Application of Nicholas Koluncich, III for Appointment to Plaintiffs' Steering Committee* by MICAELA BROWN (Attachments: # 1 Exhibit Exh. A − Firm Resume, # 2 Certificate of Service)(LaDuca, Charles) (Entered: 12/22/2015)
12/23/2015	40	NOTICE *of Corrected Application of Charles J. LaDuca for Appointment to Plaintiffs' Steering Committee* by MICAELA BROWN re 38 Notice (Other) (Attachments: # 1 Exhibit Exhibit A: Cuneo, Gilbert & LaDuca, LLP Firm Resume, # 2 Certificate of Service)(LaDuca, Charles) (Entered: 12/23/2015)
12/29/2015	41	COPY OF CONDITIONAL TRANSFER ORDER (CTO−2) dated 12/29/15 from the Judicial Panel on Multidistrict Litigation directing the transfer to the U.S. District Court for the District of Columbia with the consent of that court, assigned to the Honorable Judge Amy Berman Jackson for coordinated pretrial proceedings pursuant to 28 U.S.C. 1407.(MDL 2664)(ztnr) (Entered: 12/29/2015)
12/30/2015		MINUTE ORDER. This order relates to Binning, No. 15−cv−2259. In light of the transfer of Binning, No. 15−cv−2259, to this Court and pursuant to the Initial Practice and Procedure Order 8 entered by this Court in 15−mc−1394, In Re: U.S. Office of Personnel Management Data Security Breach Litigation, it is ORDERED that plaintiff must file by motion any objection to or request for relief from the Initial Practice and Procedure Order by January 8, 2016. It is further ORDERED that plaintiff shall file notice with the Court by January 8, 2016 stating whether he agrees to transfer his case for all purposes, waiving any right to remand under Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach, 523 U.S. 26 (1998), and 28 U.S.C.§1407(a). Signed by Judge Amy Berman Jackson on 12/30/15. (DMK) (Entered: 12/30/2015)
12/30/2015		Set/Reset Deadlines: Notice due by 1/8/2016. Motion due by 1/8/2016. (zsm) (Entered: 12/30/2015)
01/05/2016	42	RESPONSE re 26 MOTION to Appoint Counsel *(Mark Rosen) to Serve on Plaintiffs' Steering Committee* filed by WILLIAM FLEISHELL III, CHAD KAPPERS. (Attachments: # 1 Certificate of Service)(Rosen, Mark) (Entered: 01/05/2016)

01/05/2016	43	NOTICE *OF KOHN, SWIFT & GRAF, P.C. IN FURTHER SUPPORT OF ITS APPLICATION TO BE APPOINTED TO PLAINTIFFS STEERING COMMITTEE* by TERESA J. MCGARRY re 24 Notice (Other) (Attachments: # 1 Certificate of Service)(Sheils, Denis) (Entered: 01/05/2016)
01/05/2016	44	RESPONSE re 23 Notice (Other),, *in Support of Appointment of Plaintiffs' Liaison Counsel, Plaintiffs' Interim Lead Counsel and Members of the Plaintiffs' Steering Committee* filed by AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL−CIO. (Attachments: # 1 Text of Proposed Order)(Mason, Gary) (Entered: 01/05/2016)
01/05/2016	45	NOTICE OF RELATED CASE by KATHERINE ARCHULETA, JOHN BERRY, BETH F. COBERT, DOES, ELAINE D. KAPLAN, DONNA SEYMOUR, UNITED STATES DEPARTMENT OF HOMELAND SECURITY, UNITED STATES OFFICE OF PERSONNEL MANAGEMENT. Case related to Case No. 4:15−cv−5083 (N.D. Cal.). (Attachments: # 1 Exhibit Notice of Tag Along Action to JPML)(Carmichael, Andrew) (Entered: 01/05/2016)
01/05/2016	46	RESPONSE re 34 Notice (Other), 23 Notice (Other),, 31 MOTION to Appoint Counsel *John Yanchunis as Lead Class Counsel or Co−Lead Class Counsel*, 25 Notice (Other), filed by MICHAEL HANAGAN. (Attachments: # 1 Declaration of Graham B. LippSmith, # 2 Certificate of Service)(LippSmith, Graham) (Entered: 01/05/2016)
01/05/2016	47	RESPONSE re 29 Notice (Other) *Applications for Appointment to the Plaintiffs' Steering Committee* filed by VICTOR W. HOBBS. (Parekh, Behram) (Entered: 01/05/2016)
01/05/2016	48	RESPONSE re 35 Notice (Other) filed by RYAN BONNER. (Thompson, David) (Entered: 01/05/2016)
01/05/2016	49	RESPONSE *to Applications, and in Further Support of Application of Nicholas Koluncich, for Appointment to Plaintiffs' Steering Committee* filed by MICAELA BROWN. (Attachments: # 1 Certificate of Service)(LaDuca, Charles) (Entered: 01/05/2016)
01/05/2016	50	RESPONSE *to Applications, and in Further Support of Application of Charles J. LaDuca, for Appointment to Plaintiffs' Steering Committee, and Joinder in Application of Nicholas Koluncich for Appointment to Steering Committee* filed by MICAELA BROWN. (Attachments: # 1 Certificate of Service)(LaDuca, Charles) (Entered: 01/05/2016)
01/05/2016	51	RESPONSE *of Federman & Sherwood to Applications for Lead, Liaison and/or Plaintiffs' Steering Committee* filed by GARY S. COX. (Marcussen, Carin) (Entered: 01/05/2016)
01/07/2016	52	NOTICE of Appearance by Robert K. Shelquist on behalf of JERAN BINNING (Shelquist, Robert) (Entered: 01/07/2016)
01/08/2016	53	NOTICE *Plaintiff Jeran Binning's Notice of Consent to Transfer for Pretrial Purposes Without Waiving Right to Later Remand* by JERAN BINNING (Shelquist, Robert) (Entered: 01/08/2016)
01/12/2016	54	NOTICE by KATHERINE ARCHULETA, JOHN BERRY, BETH F. COBERT, DOES, ELAINE D. KAPLAN, DONNA SEYMOUR, UNITED STATES DEPARTMENT OF HOMELAND SECURITY, UNITED STATES OFFICE OF PERSONNEL MANAGEMENT (Carmichael, Andrew) (Entered: 01/12/2016)
01/19/2016	55	NOTICE *Regarding Application of Norman E. Siegel for Appointment as Interim Lead Class Counsel and Hassan Zavareei For Appointment as Liaison Counsel* by MARY C. WOO (Siegel, Norman) (Entered: 01/19/2016)
01/19/2016	56	COPY OF CONDITIONAL TRANSFER ORDER (CTO−3) dated 1/19/2016 from the Judicial Panel on Multidistrict Litigation directing the transfer to the U.S. District Court for the District of Columbia with the consent of that court, assigned to the Honorable Judge Amy Berman Jackson for coordinated pretrial proceedings pursuant to 28 U.S.C. 1407. (MDL 2664)(ztnr) (Entered: 01/21/2016)

01/21/2016		Minute Entry for Proceedings held before Judge Amy Berman Jackson: Motions Hearing held on 1/21/2016, Re: 26 31 33 Motions and Applications for Appointment as Counsel. All were Heard and Taken Under Advisement. (ORDER TO BE ISSUED) (Court Reporter: Janice Dickman) (jth) (Entered: 01/21/2016)
01/28/2016	57	TRANSCRIPT OF PROCEEDINGS before Judge Amy Berman Jackson held on January 21, 2016; Page Numbers: 1−84. Date of Issuance:January 24, 2016. Court Reporter/Transcriber Janice Dickman, Telephone number 202−354−3267, Transcripts may be ordered by submitting the Transcript Order Form.<P></P><P></P>For the first 90 days after this filing date, the transcript may be viewed at the courthouse at a public terminal or purchased from the court reporter referenced above. After 90 days, the transcript may be accessed via PACER. Other transcript formats, (multi−page, condensed, CD or ASCII) may be purchased from the court reporter.<P>**NOTICE RE REDACTION OF TRANSCRIPTS:** The parties have twenty−one days to file with the court and the court reporter any request to redact personal identifiers from this transcript. If no such requests are filed, the transcript will be made available to the public via PACER without redaction after 90 days. The policy, which includes the five personal identifiers specifically covered, is located on our website at www.dcd.uscourts.gov.<P></P> Redaction Request due 2/18/2016. Redacted Transcript Deadline set for 2/28/2016. Release of Transcript Restriction set for 4/27/2016.(Dickman, Janice) (Entered: 01/28/2016)
01/28/2016	58	ORDER appointing counsel to leadership positions for plaintiffs, setting forth time keeping requirements, and ordering that the consolidated amended complaint is due by March 14, 2016. This order relates to all cases. See order for details. Signed by Judge Amy Berman Jackson on 1/28/16. (DMK) (Entered: 01/28/2016)
01/29/2016		Set/Reset Deadline: The Consolidated Amended Complaint is due by 3/14/2016. (jth) (Entered: 01/29/2016)
02/05/2016		MINUTE ORDER. This order relates to Shamonda v. Department of Homeland Security, No. 16−cv−0178. In light of the transfer of Shamonda v. Department of Homeland Security, No. 16−cv−0178, to this Court and pursuant to the Initial Practice and Procedure Order 8 entered by this Court in 15−mc−1394, In Re: U.S. Office of Personnel Management Data Security Breach Litigation, it is ORDERED that plaintiff must file by motion any objection to or request for relief from the Initial Practice and Procedure Order by February 19, 2016. It is further ORDERED that plaintiff shall file notice with the Court by February 19, 2016 stating whether plaintiff agrees to transfer the case for all purposes, waiving any right to remand under Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach, 523 U.S. 26 (1998), and 28 U.S.C.§1407(a). Signed by Judge Amy Berman Jackson on 2/5/16. (DMK) (Entered: 02/05/2016)
02/08/2016		Set/Reset Deadlines: Pro Se Plaintiff Adedeji Shamonda (16−cv−178) must file, by motion, any objection to or request for relief from the Initial Practice and Procedure Order in case number 15−mc−1394 (Dkt. #8) by 2/19/2016, and Pro Se Plaintiff shall also file, by 2/19/2016, notice with the Court stating whether Pro Se Plaintiff agrees to transfer the case for all purposes, waiving any right to remand under Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach, 523 U.S. 26 (1998), and 28 U.S.C.§1407(a). (jth) (Entered: 02/08/2016)
02/12/2016	59	NOTICE OF RELATED CASE by KATHERINE ARCHULETA, JOHN BERRY, BETH F. COBERT, DOES, ELAINE D. KAPLAN, DONNA SEYMOUR, UNITED STATES DEPARTMENT OF HOMELAND SECURITY, UNITED STATES OFFICE OF PERSONNEL MANAGEMENT. Case related to Case No. CAN 3:16−543. (Attachments: # 1 Exhibit)(Carmichael, Andrew) (Entered: 02/12/2016)
02/25/2016	60	COPY OF CONDITIONAL TRANSFER ORDER (CTO−4) dated 2/25/16 from the Judicial Panel on Multidistrict Litigation directing the transfer to the U.S. District Court for the District of Columbia with the consent of that court, assigned to the Honorable Judge Amy Berman Jackson for coordinated pretrial proceedings pursuant to 28 U.S.C. 1407. (MDL 2664)(ztnr) (Entered: 02/25/2016)
02/26/2016	61	NOTICE TO THE COURT by ADEDEJI SHAMONDA (jf) (Entered: 02/29/2016)
02/29/2016		MINUTE ORDER. This order relates to Shamonda v. Department of Homeland Security, No. 16−cv−0392. In light of the transfer of Shamonda v. Department of

		Homeland Security, No. 16−cv−00392, to this Court and pursuant to the Initial Practice and Procedure Order 8 entered by this Court in 15−mc−1394, In Re: U.S. Office of Personnel Management Data Security Breach Litigation, it is ORDERED that plaintiff must file by motion any objection to or request for relief from the Initial Practice and Procedure Order by March 14, 2016. It is further ORDERED that plaintiff shall file notice with the Court by March 14, 2016 stating whether plaintiff agrees to transfer the case for all purposes, waiving any right to remand under Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach, 523 U.S. 26 (1998), and 28 U.S.C.§1407(a). Signed by Judge Amy Berman Jackson on 2/29/16. (DMK) Modified on 3/1/2016 to reflect that this is a minute (paperless) order (jth). (Entered: 02/29/2016)
03/01/2016		Set/Reset Deadlines: Pro Se Plaintiff Adebiyi K. Shamonda (16−cv−392) must file, by motion, any objection to or request for relief from the Initial Practice and Procedure Order in case number 15−mc−1394 (Dkt. #8) by 3/14/2016, and Pro Se Plaintiff shall also file, by 3/14/2016, notice with the Court stating whether Pro Se Plaintiff agrees to transfer the case for all purposes, waiving any right to remand under Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach, 523 U.S. 26 (1998), and 28 U.S.C.§1407(a). (jth) (Entered: 03/01/2016)
03/03/2016	62	NOTICE OF WITHDRAWAL OF APPEARANCE as to KATHERINE ARCHULETA, JOHN BERRY, BETH F. COBERT, ELAINE D. KAPLAN, DONNA SEYMOUR, UNITED STATES DEPARTMENT OF HOMELAND SECURITY, UNITED STATES OFFICE OF PERSONNEL MANAGEMENT. Attorney Paul G. Freeborne terminated. (Freeborne, Paul) (Entered: 03/03/2016)
03/14/2016	63	AMENDED COMPLAINT against KEYPOINT GOVERNMENT SOLUTIONS, UNITED STATES OFFICE OF PERSONNEL MANAGEMENT with Jury Demand filed by RYAN BONNER, MICHAEL HANAGAN, TERESA J. MCGARRY, ROBERT CRAWFORD, AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL−CIO, MARIO SAMPEDRO, GARDELL BRANCH, ROBERT SLATER, JANE DOE II, TORALF PETERS, MYRNA BROWN, CHARLENE OLIVER, DARREN STRICKLAND, CYNTHIA KING−MYERS, TRAVIS ARNOLD, MICHAEL JOHNSON, TONY BACHTELL, ZACHARY SHARPER, JENNIFER GUM, JOHN DOE III, JOHN DOE II, JOHN DOE, MICHAEL EBERT, DEBORAH HOFFMAN, PAUL DALY, LILLIAN GONZALEZ−COLON, KELLY FLYNN, PETER ULIANO, RYAN LOZAR, ORIN GRIFFITH, TIMOTHY SEBERT, JOHNNY GONZALEZ, MARYANN HIBBS, ALIA FULI, HEATHER BURNETT−RICK, MONTY BOS, JANE DOE, NANCY WHEATLEY, KIMBERLY WINSOR.(Girard, Daniel) (Entered: 03/14/2016)
03/15/2016		MINUTE ORDER. This order relates to all cases. Pursuant to the Court's orders of December 15, 2015 and January 28, 2016, it is ORDERED that motions to dismiss the consolidated amended complaint and the NTEU complaint are due May 13, 2016, oppositions are due June 27, 2016, and replies are due July 18, 2016. Signed by Judge Amy Berman Jackson on 3/15/16.(DMK) (Entered: 03/15/2016)
03/17/2016		Set/Reset Deadlines: Motions to Dismiss the Consolidated Amended Complaint, and the NTEU Complaint are due 5/13/2016, Oppositions are due 6/27/2016, Replies are due 7/18/2016. (jth) (Entered: 03/17/2016)
03/18/2016	64	NOTICE by ADEBIYI K. SHAMONDA re Minute Order filed on 03/01/2016 (jf) (Entered: 03/22/2016)
03/24/2016		MINUTE ORDER. This order relates to Adedeji Shamonda v. Department of Homeland Security, No. 16−0178, and Adebiyi Shamonda v. Department of Homeland Security, No. 16−0392. In light of waiver of the right to remand under 28 U.S.C. § 1407 and Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach, 523 U.S. 26 (1998), filed by plaintiffs [Dkt. # 61 and #64], the consolidated amended complaint [Dkt. # 63] will serve as the superseding, operative complaint in the following additional cases: Adedeji Shamonda v. Department of Homeland Security, No. 16−0178, and Adebiyi Shamonda v. Department of Homeland Security, No. 16−0392. Signed by Judge Amy Berman Jackson on 3/24/16. (DMK) (Entered: 03/24/2016)
04/08/2016	65	NOTICE of Change of Address by Richard Henry Gordin (Gordin, Richard) (Entered: 04/08/2016)

04/11/2016		NOTICE OF ERROR re 65 Notice of Change of Address; emailed to rhg@girardgibbs.com, cc'd 94 associated attorneys −− The PDF file you docketed contained errors: 1. You must file a notice of apperance (jf,) (Entered: 04/11/2016)
04/21/2016	66	NOTICE of Appearance by Steven William Teppler on behalf of JOHN ORAVIS, HECTOR PEREZ (Teppler, Steven) (Entered: 04/21/2016)
04/26/2016	67	NOTICE of Appearance by Kieran Gavin Gostin on behalf of KATHERINE ARCHULETA, JOHN BERRY, BETH F. COBERT, ELAINE D. KAPLAN, DONNA SEYMOUR, UNITED STATES DEPARTMENT OF HOMELAND SECURITY, UNITED STATES OFFICE OF PERSONNEL MANAGEMENT (Gostin, Kieran) (Entered: 04/26/2016)
05/03/2016	68	MOTION for Leave to File Excess Pages *for Memorandum in Support of Motion to Dismiss the Consolidated Amended Complaint* by KATHERINE ARCHULETA (Attachments: # 1 Text of Proposed Order)(Josephson, Matthew) (Entered: 05/03/2016)
05/04/2016	69	NOTICE of Change of Address by Gary Edward Mason (Mason, Gary) (Entered: 05/04/2016)
05/04/2016		MINUTE ORDER granting in part and denying in part 68 Unopposed Motion for Leave to File Excess Pages. This order relates to all cases except NTEU v. Cobert, 15−cv−1808−ABJ (D.D.C.). The federal defendant is granted leave to file a memorandum of no more than 70 pages in support of its motion to dismiss the three substantive counts against it and that portion of Count 4 that applies to it. The Court notes that any footnotes in the memorandum, like the rest of the memorandum, must be in 12 point font. Signed by Judge Amy Berman Jackson on 5/4/16. (DMK) (Entered: 05/04/2016)
05/13/2016	70	MOTION to Dismiss by KEYPOINT GOVERNMENT SOLUTIONS (Attachments: # 1 Appendix A, # 2 Exhibit A, # 3 Exhibit B, # 4 Text of Proposed Order)(Warin, Francis) (Entered: 05/13/2016)
05/13/2016	71	Corporate Disclosure Statement by KEYPOINT GOVERNMENT SOLUTIONS. (Warin, Francis) (Entered: 05/13/2016)
05/13/2016	72	MOTION to Dismiss *the Consolidated Amended Complaint* by KATHERINE ARCHULETA (Attachments: # 1 Memorandum in Support, # 2 Exhibit 1 − OPM Announcement (June 5, 2015), # 3 Exhibit 2 − OPM Announcement (July 9, 2015), # 4 Exhibit 3 − Chart of Plaintiff's Alleged Damages)(Josephson, Matthew) (Entered: 05/13/2016)
05/13/2016	73	MOTION to Dismiss *the NTEU Complaint* by KATHERINE ARCHULETA (Attachments: # 1 Memorandum in Support, # 2 Text of Proposed Order)(Josephson, Matthew) (Entered: 05/13/2016)
05/17/2016		MINUTE ORDER. This order relates to all cases. It is ORDERED that liaison counsel shall confer with interim lead class counsel, other plaintiffs' counsel, and defense counsel and file a notice listing all of the dates from the following list on which the parties would be available for a hearing on OPM's motion to dismiss and/or Keypoint's motion to dismiss the consolidated amended complaint: August 9, 10, 11, 30, 31; September 1; October 26, 27, 28; and November 4, 8, 9, and 10. The Court will schedule the hearing on OPM's motion to dismiss the NTEU complaint separately. Signed by Judge Amy Berman Jackson on 5/17/16. (DMK) (Entered: 05/17/2016)
05/18/2016		MINUTE ORDER. This order relates to all cases. The notice required by the minute order issued on May 17, 2016 shall be filed by May 27, 2016. SO ORDERED. Signed by Judge Amy Berman Jackson on 05/18/2016. (zjth) (Entered: 05/18/2016)
05/27/2016	74	NOTICE *of Proposed Hearing Dates* by AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL−CIO, TRAVIS ARNOLD, TONY BACHTELL, JERAN BINNING, RYAN BONNER, MONTY BOS, GARDELL BRANCH, MICAELA BROWN, MYRNA BROWN, HEATHER BURNETT−RICK, NICHOLAS D. CAVIS, GARY S. COX, ROBERT CRAWFORD, ADAM DALE, PAUL DALY, JANE DOE, JOHN DOE, JANE DOE II, JOHN DOE II, JOHN DOE III, MICHAEL EBERT, ERIC W. EDGAR, WILLIAM FLEISHELL III, KELLY FLYNN, ALIA FULI, JOHNNY GONZALEZ, LILLIAN GONZALEZ−COLON,

		ORIN GRIFFITH, JENNIFER GUM, MICHAEL HANAGAN, MARYANN HIBBS, VICTOR W. HOBBS, DEBORAH HOFFMAN, STEPHEN HOWELL, IN RE: U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION, MICHAEL JOHNSON, CHAD KAPPERS, CYNTHIA KING−MYERS, EDWARD W. KRIPPENDORF, RYAN LOZAR, TERESA J. MCGARRY, NATIONAL TREASURY EMPLOYEES UNION, CHARLENE OLIVER, JOHN ORAVIS, JOHN ORTINO, HECTOR PEREZ, TORALF PETERS, WILLIAM PRESTON, JOHN RABER, EDWARD L. ROBBELOTH, MARIO SAMPEDRO, TIMOTHY SEBERT, ADEBIYI K. SHAMONDA, ADEDEJI SHAMONDA, ZACHARY SHARPER, DERRICK SIMS, ROBERT SLATER, HOWARD SMITH, DARREN STRICKLAND, PETER ULIANO, NICOLE WAID, NANCY WHEATLEY, KIMBERLY WINSOR, MARY C. WOO re Order,, Order, Set Deadlines (Mason, Gary) (Entered: 05/27/2016)
06/03/2016	75	AMENDED COMPLAINT against BETH F. COBERT filed by NATIONAL TREASURY EMPLOYEES UNION.(Shah, Paras) (Entered: 06/03/2016)
06/03/2016	76	NOTICE *Regarding Filing of Amended Complaint* by NATIONAL TREASURY EMPLOYEES UNION (Shah, Paras) (Entered: 06/03/2016)
06/07/2016		MINUTE ORDER. This order relates to all cases except NTEU v. Cobert, 15−cv−1808−ABJ (D.D.C.). In light of the notice of proposed hearing dates 74 , a hearing on OPM's motion to dismiss 72 and KeyPoint's motion to dismiss 70 is scheduled for October 27, 2016 at 10:00 a.m., and the hearing will continue on November 10, 2016 at 10:00 a.m. Signed by Judge Amy Berman Jackson on 6/7/16. (DMK) (Entered: 06/07/2016)
06/07/2016		MINUTE ORDER. This order relates to NTEU v. Cobert, 15−cv−1808−ABJ (D.D.C.), denying as moot 73 Federal Defendant's Motion to Dismiss the NTEU Plaintiffs' Complaint. In light of the amended complaint filed by the NTEU plaintiffs 75 , federal defendant's motion to dismiss is denied as moot. Federal defendant shall answer or otherwise respond to the amended complaint by June 21, 2016. Signed by Judge Amy Berman Jackson on 6/7/16. (DMK) (Entered: 06/07/2016)
06/09/2016		Set/Reset Hearings: Hearing on OPM's Motion to Dismiss 72 and KeyPoint's Motion to Dismiss 70 is scheduled for 10/27/2016 at 10:00 AM, and the hearing will continue on 11/10/2016 at 10:00 AM. (jth) (Entered: 06/09/2016)
06/15/2016	77	Joint MOTION for Briefing Schedule by KATHERINE ARCHULETA, BETH F. COBERT, DONNA SEYMOUR, UNITED STATES OFFICE OF PERSONNEL MANAGEMENT (Attachments: # 1 Text of Proposed Order)(Josephson, Matthew) (Entered: 06/15/2016)
06/16/2016		MINUTE ORDER granting 77 Motion to Modify Briefing Schedule. This order relates to all cases. It is ORDERED that the government's anticipated motion to dismiss the amended complaint in National Treasury Employees Union v. Colbert, 15−cv−1808−ABJ, is due June 27, 2016; plaintiff's opposition is due July 27, 2016; and the government's reply is due August 29, 2016. It is further ORDERED that plaintiffs' oppositions to defendants' motions to dismiss the consolidated amended complaint are due June 30, 2016 and defendants' replies are due August 3, 2016. Signed by Judge Amy Berman Jackson on 6/16/16. (DMK) (Entered: 06/16/2016)
06/17/2016		Set/Reset Deadlines: The Government's anticipated Motion to Dismiss the Amended Complaint in NTEU v. Colbert, 15−cv−1808 (ABJ) is due 6/27/2016; Plaintiff's Opposition is due 7/27/2016; the Government's Reply is due 8/29/2016. Plaintiffs' Oppositions to Defendants' Motions to Dismiss the Consolidated Amended Complaint are due by 6/30/2016; Defendants' Replies are due by 8/3/2016. (jth) (Entered: 06/17/2016)
06/17/2016	78	COPY OF CONDITIONAL TRANSFER ORDER (CTO−5) dated 6/17/16 from the Judicial Panel on Multidistrict Litigation directing the transfer to the U.S. District Court for the District of Columbia with the consent of that court, assigned to the Honorable Judge Amy Berman Jackson for coordinated pretrial proceedings pursuant to 28 U.S.C. 1407.(MDL 2664) (ztnr) (Entered: 06/20/2016)
06/21/2016		MINUTE ORDER. This order relates to Golden v. U.S. Office of Personnel Management, 16−cv−1253. In light of the transfer of Golden v. U.S. Office of

		Personnel Management to this Court and pursuant to the Initial Practice and Procedure Order 8 entered by this Court in 15−mc−1394, In Re: U.S. Office of Personnel Management Data Security Breach Litigation, it is ORDERED that plaintiffs must file by motion any objection to or request for relief from the Initial Practice and Procedure Order by July 5, 2016. It is further ORDERED that plaintiffs shall file notice with the Court by July 5, 2016 stating whether plaintiffs agree to transfer the case for all purposes, waiving any right to remand under Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach, 523 U.S. 26 (1998), and 28 U.S.C.§1407(a). Signed by Judge Amy Berman Jackson on 6/21/16. (DMK) (Entered: 06/21/2016)
06/21/2016	79	MOTION for Leave to File *Excess Pages for Memorandum in Support of Consolidated Opposition to Defendants' Motions to Dismiss the Consolidated Amended Complaint* by AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL−CIO, TRAVIS ARNOLD, TONY BACHTELL, RYAN BONNER, MONTY BOS, GARDELL BRANCH, MYRNA BROWN, HEATHER BURNETT−RICK, ROBERT CRAWFORD, PAUL DALY, JANE DOE, JOHN DOE, JANE DOE II, JOHN DOE II, JOHN DOE III, MICHAEL EBERT, KELLY FLYNN, ALIA FULI, JOHNNY GONZALEZ, LILLIAN GONZALEZ−COLON, ORIN GRIFFITH, JENNIFER GUM, MICHAEL HANAGAN, MARYANN HIBBS, DEBORAH HOFFMAN, MICHAEL JOHNSON, CYNTHIA KING−MYERS, RYAN LOZAR, TERESA J. MCGARRY, CHARLENE OLIVER, TORALF PETERS, MARIO SAMPEDRO, TIMOTHY SEBERT, ZACHARY SHARPER, ROBERT SLATER, DARREN STRICKLAND, PETER ULIANO, NANCY WHEATLEY, KIMBERLY WINSOR (Attachments: # 1 Text of Proposed Order)(Girard, Daniel) (Entered: 06/21/2016)
06/21/2016		Set/Reset Deadlines: Plaintiffs' in 16−cv−1253, Golden v. OPM, must file by motion any objection to or request for relief from the Initial Practice and Procedure Order by 7/5/2016. Plaintiffs shall also file notice with the Court by 7/5/2016 stating whether they agree to transfer the case for all purposes, waiving any right to remand under Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach, 523 U.S. 26 (1998), and 28 U.S.C.§1407(a). (jth) (Entered: 06/22/2016)
06/22/2016		MINUTE ORDER granting 79 unopposed motion for leave to file. This order relates to all cases except NTEU v. Cobert, 15−cv−1808−ABJ (D.D.C.). It is ORDERED that plaintiffs are permitted to file a consolidated opposition to defendants' motions to dismiss the consolidated amended complaint, which shall not exceed 110 pages. Signed by Judge Amy Berman Jackson on 6/22/16. (DMK) (Entered: 06/22/2016)
06/22/2016	80	NOTICE of Appearance by Joseph Evan Borson on behalf of KATHERINE ARCHULETA, BETH F. COBERT, DONNA SEYMOUR, UNITED STATES OFFICE OF PERSONNEL MANAGEMENT (Borson, Joseph) (Entered: 06/22/2016)
06/27/2016	81	MOTION to Dismiss *NTEU Plaintiffs' Amended Complaint* by BETH F. COBERT (Attachments: # 1 Memorandum in Support, # 2 Text of Proposed Order)(Josephson, Matthew) (Entered: 06/27/2016)
06/30/2016	82	Memorandum in opposition to re 70 MOTION to Dismiss , 72 MOTION to Dismiss *the Consolidated Amended Complaint* filed by AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL−CIO, TRAVIS ARNOLD, TONY BACHTELL, RYAN BONNER, MONTY BOS, GARDELL BRANCH, MYRNA BROWN, HEATHER BURNETT−RICK, ROBERT CRAWFORD, PAUL DALY, JANE DOE, JOHN DOE, JANE DOE II, JOHN DOE II, JOHN DOE III, MICHAEL EBERT, KELLY FLYNN, ALIA FULI, JOHNNY GONZALEZ, LILLIAN GONZALEZ−COLON, ORIN GRIFFITH, JENNIFER GUM, MICHAEL HANAGAN, MARYANN HIBBS, DEBORAH HOFFMAN, MICHAEL JOHNSON, CYNTHIA KING−MYERS, RYAN LOZAR, TERESA J. MCGARRY, CHARLENE OLIVER, TORALF PETERS, MARIO SAMPEDRO, TIMOTHY SEBERT, ZACHARY SHARPER, ROBERT SLATER, DARREN STRICKLAND, PETER ULIANO, NANCY WHEATLEY, KIMBERLY WINSOR. (Attachments: # 1 Appendix, # 2 Text of Proposed Order)(Girard, Daniel) (Entered: 06/30/2016)
07/14/2016		MINUTE ORDER. This order relates to Golden v. OPM, 16−cv−1253. On June 21, 2016, the Court ordered plaintiffs in that case to file by July 5, 2016 any objection or request for relief from the Initial Practice and Procedure Order and notice of their position on waiver of remand. Receiving no filing from plaintiffs by the deadline, the

		Court notes that plaintiffs are bound by the Initial Practice and Procedure Order 8 . Further, it is ORDERED that plaintiffs shall file notice by July 25, 2016 stating whether they agree to transfer the case for all purposes, waiving any right to remand under Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach, 523 U.S. 26 (1998), and 28 U.S.C.§1407(a). Signed by Judge Amy Berman Jackson on 7/14/16. (DMK) (Entered: 07/14/2016)
07/14/2016		Set/Reset Deadlines: This relates to Golden v. OPM, case No. 16−cv−1253. Plaintiffs shall file notice by 7/25/2016 stating whether they agree to transfer the case for all purposes, waiving any right to remand under Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach, 523 U.S. 26 (1998), and 28 U.S.C.§1407(a). (jth) (Entered: 07/14/2016)
07/27/2016	83	MOTION for Leave to File Excess Pages by UNITED STATES OFFICE OF PERSONNEL MANAGEMENT (Attachments: # 1 Text of Proposed Order)(Josephson, Matthew) (Entered: 07/27/2016)
07/27/2016	84	Memorandum in opposition to re 81 MOTION to Dismiss *NTEU Plaintiffs' Amended Complaint* filed by EUGENE GAMBARDELLA, STEPHEN HOWELL, NATIONAL TREASURY EMPLOYEES UNION, JOHN ORTINO. (Attachments: # 1 Text of Proposed Order)(Shah, Paras) (Entered: 07/27/2016)
07/27/2016		MINUTE ORDER granting 83 defendant OPM's unopposed motion for leave to file excess pages. This order relates to all cases except NTEU v. Cobert, 15−cv−1808−ABJ (D.D.C.). It is ORDERED that OPM is permitted to file a reply not to exceed 35 pages in support of its motion to dismiss the Consolidated Amended Complaint. Signed by Judge Amy Berman Jackson on 7/27/16. (DMK) (Entered: 07/27/2016)
07/27/2016	85	MOTION for Leave to File Excess Pages by KEYPOINT GOVERNMENT SOLUTIONS (Attachments: # 1 Text of Proposed Order)(Mendro, Jason) (Entered: 07/27/2016)
07/27/2016		MINUTE ORDER granting 85 KeyPoint's unopposed motion for leave to file excess pages. This order relates to all cases except NTEU v. Cobert, 15−cv−1808−ABJ (D.D.C.). It is ORDERED that KeyPoint is permitted to file a reply not to exceed 35 pages in support of its motion to dismiss the Consolidated Amended Complaint. It is FURTHER ORDERED that the reply briefs of both defendants should not repeat arguments set forth in their initial briefs. Signed by Judge Amy Berman Jackson on 7/27/16. (DMK) (Entered: 07/27/2016)
08/01/2016		MINUTE ORDER. This order relates to Golden v. OPM, 16−cv−1253. The Court has twice ordered plaintiffs to notify the Court whether they agree to transfer the case to this Court for all purposes and to waive their right to remand to the N.D. of Alabama upon completion of the pretrial proceedings. See Minute Orders of June 21, 2016 and July 14, 2016. Both times, plaintiffs have failed to respond. Therefore, it is ORDERED that if plaintiffs in Golden v. OPM, 16−cv−1253 object to the transfer of the the case to this district for all purposes, and wish to assert their right to remand under Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach, 523 U.S. 26 (1998), and 28 U.S.C.§1407(a), they must notify the Court by August 8, 2016. Failure to note an objection by that date may be deemed to be a waiver of plaintiffs' right to remand. Signed by Judge Amy Berman Jackson on 8/1/16.(DMK) (Entered: 08/01/2016)
08/01/2016		Set/Reset Deadlines: This relates to Golden v. OPM, case No. 16−cv−1253. Plaintiffs shall file notice by 8/8/2016 stating whether they agree to transfer the case for all purposes, waiving any right to remand under Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach, 523 U.S. 26 (1998), and 28 U.S.C.§1407(a). (jth) (Entered: 08/01/2016)
08/02/2016		MINUTE ORDER. This order relates to ALL CASES. It is ORDERED that there will be hearing on defendant's motion to dismiss the NTEU complaint 81 on October 27, 2016 at 10:00 a.m. when the motions related to the consolidated amended complaint are already scheduled to be heard. Counsel are advised that this hearing will address the standing and jurisdictional issues raised in Section I of OPM's memorandum [72−1] at 16−37, and Section I of KeyPoint's memorandum 70 at 6−17, as well as Section I of defendant's memorandum in support of the motion to dismiss the NTEU complaint [81−1] at 6−14. The Court will also hear argument on Section II of OPM's

		argument concerning the failure to plead actual damages under the Privacy Act [72−1] at 37−42, and Section II of KeyPoint's argument concerning government contractor immunity 70 at 17−22. Signed by Judge Amy Berman Jackson on 8/2/16.(DMK) (Entered: 08/02/2016)
08/03/2016	86	REPLY to opposition to motion re 70 MOTION to Dismiss filed by KEYPOINT GOVERNMENT SOLUTIONS. (Attachments: # 1 Appendix A)(Warin, Francis) (Entered: 08/03/2016)
08/03/2016	87	REPLY to opposition to motion re 72 MOTION to Dismiss *the Consolidated Amended Complaint* filed by UNITED STATES OFFICE OF PERSONNEL MANAGEMENT. (Josephson, Matthew) (Entered: 08/03/2016)
08/08/2016	88	NOTICE of Appearance by Eric J. Artrip on behalf of DAVID A. GOLDEN, LILIANA GOLDEN, RONNIE GOLDEN (Artrip, Eric) (Entered: 08/08/2016)
08/08/2016	89	NOTICE *of Election* by DAVID A. GOLDEN, LILIANA GOLDEN, RONNIE GOLDEN re Order,,, Set/Reset Deadlines, Order,,, (Artrip, Eric) (Entered: 08/08/2016)
08/23/2016	90	NOTICE OF SUPPLEMENTAL AUTHORITY by UNITED STATES OFFICE OF PERSONNEL MANAGEMENT (Attachments: # 1 Exhibit Opinion in Attias v. CareFirst)(Carmichael, Andrew) (Entered: 08/23/2016)
08/29/2016	91	REPLY to opposition to motion re 81 MOTION to Dismiss *NTEU Plaintiffs' Amended Complaint* filed by UNITED STATES OFFICE OF PERSONNEL MANAGEMENT. (Carmichael, Andrew) (Entered: 08/29/2016)
09/16/2016	92	NOTICE OF SUPPLEMENTAL AUTHORITY by EUGENE GAMBARDELLA, STEPHEN HOWELL, NATIONAL TREASURY EMPLOYEES UNION, JOHN ORTINO (Attachments: # 1 Exhibit)(Shah, Paras) (Entered: 09/16/2016)
10/05/2016	93	NOTICE OF SUPPLEMENTAL AUTHORITY by EUGENE GAMBARDELLA, STEPHEN HOWELL, NATIONAL TREASURY EMPLOYEES UNION, JOHN ORTINO (Attachments: # 1 Exhibit)(Shah, Paras) (Entered: 10/05/2016)
10/13/2016	94	NOTICE by EUGENE GAMBARDELLA, STEPHEN HOWELL, NATIONAL TREASURY EMPLOYEES UNION, JOHN ORTINO (Shah, Paras) (Entered: 10/13/2016)
10/17/2016	95	NOTICE OF SUPPLEMENTAL AUTHORITY by AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL−CIO, TRAVIS ARNOLD, TONY BACHTELL, RYAN BONNER, MONTY BOS, GARDELL BRANCH, MYRNA BROWN, HEATHER BURNETT−RICK, ROBERT CRAWFORD, PAUL DALY, JANE DOE, JOHN DOE, JANE DOE II, JOHN DOE II, JOHN DOE III, MICHAEL EBERT, KELLY FLYNN, ALIA FULI, JOHNNY GONZALEZ, LILLIAN GONZALEZ−COLON, ORIN GRIFFITH, JENNIFER GUM, MICHAEL HANAGAN, MARYANN HIBBS, DEBORAH HOFFMAN, MICHAEL JOHNSON, CYNTHIA KING−MYERS, RYAN LOZAR, TERESA J. MCGARRY, CHARLENE OLIVER, TORALF PETERS, MARIO SAMPEDRO, TIMOTHY SEBERT, ZACHARY SHARPER, ROBERT SLATER, DARREN STRICKLAND, PETER ULIANO, NANCY WHEATLEY, KIMBERLY WINSOR (Attachments: # 1 Exhibit 1, # 2 Exhibit 2, # 3 Exhibit 3, # 4 Exhibit 4, # 5 Exhibit 5, # 6 Exhibit 6)(Girard, Daniel) (Entered: 10/17/2016)
10/27/2016		Minute Entry for proceedings held before Judge Amy Berman Jackson: Motions Hearing begun and held on 10/27/2016 re: 70 Motion to Dismiss filed by KEYPOINT GOVERNMENT SOLUTIONS; 72 Motion to Dismiss *the Consolidated Amended Complaint* filed by KATHERINE ARCHULETA, 81 Motion to Dismiss *NTEU Plaintiffs' Amended Complaint* filed by BETH F. COBERT. Motions Hearing continued to 11/10/2016 at 9:30 AM in Courtroom 3 before Judge Amy Berman Jackson. (Court Reporter: Janice Dickman) (jth) (Entered: 10/27/2016)
10/27/2016	96	NOTICE of Appearance by Peter A. Patterson on behalf of RYAN BONNER (Patterson, Peter) (Entered: 10/27/2016)
10/28/2016	97	NOTICE OF WITHDRAWAL OF APPEARANCE as to UNITED STATES OFFICE OF PERSONNEL MANAGEMENT. Attorney Kieran Gavin Gostin terminated.

		(Josephson, Matthew) (Entered: 10/28/2016)
10/31/2016	98	TRANSCRIPT OF PROCEEDINGS before Judge Amy Berman Jackson held on October 27, 2016; Page Numbers: 1−112. Date of Issuance:October 31, 2016. Court Reporter/Transcriber Janice Dickman, Telephone number 202−354−3267, Transcripts may be ordered by submitting the Transcript Order Form For the first 90 days after this filing date, the transcript may be viewed at the courthouse at a public terminal or purchased from the court reporter r eferenced above. After 90 days, the transcript may be accessed via PACER. Other transcript formats, (multi−page, condensed, CD or ASCII) may be purchased from the court reporter. **NOTICE RE REDACTION OF TRANSCRIPTS:** The parties have twenty−one days to file with the court and the court reporter any request to redact personal identifiers from this transcript. If no such requests are filed, the transcript will be made available to the public via PACER without redaction after 90 days. The policy, which includes the five personal identifiers specifically covered, is located on our website at www.dcd.uscourts.gov. Redaction Request due 11/21/2016. Redacted Transcript Deadline set for 12/1/2016. Release of Transcript Restriction set for 1/29/2017.(Dickman, Janice) (Entered: 10/31/2016)
11/02/2016		MINUTE ORDER. This Order relates to all cases. It is ORDERED that all parties, including plaintiffs in the NTEU case, may appear at the November 10, 2016 hearing to argue other issues raised in the motions to dismiss that were not argued at the October 27, 2016 hearing. Signed by Judge Amy Berman Jackson on 11/2/16. (DMK) (Entered: 11/02/2016)
11/03/2016	99	NOTICE *OF RECENT DECISION* by KATHERINE ARCHULETA, JOHN BERRY, BETH F. COBERT, IN RE: U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION, ELAINE D. KAPLAN (Attachments: # 1 Exhibit A − Welborn v. IRS (D.D.C. Nov. 2, 2016))(Borson, Joseph) (Entered: 11/03/2016)
11/07/2016	100	NOTICE of Appearance by Patrick A. Barthle, II on behalf of HECTOR PEREZ (Barthle, Patrick) (Entered: 11/07/2016)
11/07/2016	101	NOTICE of Appearance by John Yanchunis on behalf of HECTOR PEREZ (Yanchunis, John) (Entered: 11/07/2016)
11/08/2016	102	NOTICE *of Supplemental Citations* by KEYPOINT GOVERNMENT SOLUTIONS (Mendro, Jason) (Entered: 11/08/2016)
11/09/2016	103	RESPONSE re 102 Notice (Other) *of Supplemental Citations* filed by AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL−CIO, TRAVIS ARNOLD, TONY BACHTELL, RYAN BONNER, MONTY BOS, GARDELL BRANCH, MYRNA BROWN, HEATHER BURNETT−RICK, ROBERT CRAWFORD, PAUL DALY, JANE DOE, JOHN DOE, JANE DOE II, JOHN DOE II, JOHN DOE III, MICHAEL EBERT, KELLY FLYNN, ALIA FULI, JOHNNY GONZALEZ, LILLIAN GONZALEZ−COLON, ORIN GRIFFITH, JENNIFER GUM, MICHAEL HANAGAN, MARYANN HIBBS, DEBORAH HOFFMAN, MICHAEL JOHNSON, CYNTHIA KING−MYERS, RYAN LOZAR, TERESA J. MCGARRY, CHARLENE OLIVER, TORALF PETERS, MARIO SAMPEDRO, TIMOTHY SEBERT, ZACHARY SHARPER, ROBERT SLATER, DARREN STRICKLAND, PETER ULIANO, NANCY WHEATLEY, KIMBERLY WINSOR. (Girard, Daniel) (Entered: 11/09/2016)
11/10/2016		Minute Entry for Proceedings held before Judge Amy Berman Jackson: Motions Hearing held on 11/10/2016 re: KEYPOINT GOVERNMENT SOLUTIONS 70 MOTION to Dismiss, and The Government's 72 MOTION to Dismiss *the Consolidated Amended Complaint*, and 81 MOTION to Dismiss *NTEU Plaintiffs' Amended Complaint*. All Motions 70 , 72 , and 81 were Heard and Taken Under Advisement. (Court Reporter: Janice Dickman) (jth) (Entered: 11/10/2016)
11/16/2016	104	TRANSCRIPT OF PROCEEDINGS before Judge Amy Berman Jackson held on November 10, 2016; Page Numbers: 1−84. Date of Issuance: November 14, 2016.

		Court Reporter/Transcriber Janice Dickman, Telephone number 202−354−3267, Transcripts may be ordered by submitting the Transcript Order Form<P></P><P></P>For the first 90 days after this filing date, the transcript may be viewed at the courthouse at a public terminal or purchased from the court reporter referenced above. After 90 days, the transcript may be accessed via PACER. Other transcript formats, (multi−page, condensed, CD or ASCII) may be purchased from the court reporter.<P>**NOTICE RE REDACTION OF TRANSCRIPTS:** The parties have twenty−one days to file with the court and the court reporter any request to redact personal identifiers from this transcript. If no such requests are filed, the transcript will be made available to the public via PACER without redaction after 90 days. The policy, which includes the five personal identifiers specifically covered, is located on our website at www.dcd.uscourts.gov.<P></P> Redaction Request due 12/7/2016. Redacted Transcript Deadline set for 12/17/2016. Release of Transcript Restriction set for 2/14/2017.(Dickman, Janice) (Entered: 11/16/2016)
12/15/2016	105	NOTICE OF WITHDRAWAL OF APPEARANCE as to UNITED STATES OFFICE OF PERSONNEL MANAGEMENT. Attorney Matthew A. Josephson terminated. (Josephson, Matthew) (Entered: 12/15/2016)
01/23/2017	106	NOTICE OF SUPPLEMENTAL AUTHORITY by EUGENE GAMBARDELLA, STEPHEN HOWELL, NATIONAL TREASURY EMPLOYEES UNION, JOHN ORTINO (Attachments: # 1 Exhibit)(Shah, Paras) (Entered: 01/23/2017)
01/26/2017	107	RESPONSE re 106 NOTICE OF SUPPLEMENTAL AUTHORITY filed by UNITED STATES OFFICE OF PERSONNEL MANAGEMENT. (Carmichael, Andrew) (Entered: 01/26/2017)
01/30/2017	108	RESPONSE re 106 NOTICE OF SUPPLEMENTAL AUTHORITY filed by KEYPOINT GOVERNMENT SOLUTIONS. (Mendro, Jason) (Entered: 01/30/2017)
02/08/2017	109	NOTICE OF SUPPLEMENTAL AUTHORITY by UNITED STATES OFFICE OF PERSONNEL MANAGEMENT (Attachments: # 1 Exhibit Ex. A − Beck v. McDonald)(Borson, Joseph) (Entered: 02/08/2017)
02/09/2017	110	RESPONSE re 109 NOTICE OF SUPPLEMENTAL AUTHORITY filed by EUGENE GAMBARDELLA, STEPHEN HOWELL, NATIONAL TREASURY EMPLOYEES UNION, JOHN ORTINO. (Shah, Paras) (Entered: 02/09/2017)
08/01/2017	111	NOTICE OF SUPPLEMENTAL AUTHORITY by AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL−CIO, TRAVIS ARNOLD, TONY BACHTELL, RYAN BONNER, MONTY BOS, GARDELL BRANCH, MYRNA BROWN, HEATHER BURNETT−RICK, ROBERT CRAWFORD, PAUL DALY, JANE DOE, JOHN DOE, JANE DOE II, JOHN DOE II, JOHN DOE III, MICHAEL EBERT, KELLY FLYNN, ALIA FULI, JOHNNY GONZALEZ, LILLIAN GONZALEZ−COLON, ORIN GRIFFITH, JENNIFER GUM, MICHAEL HANAGAN, MARYANN HIBBS, DEBORAH HOFFMAN, MICHAEL JOHNSON, CYNTHIA KING−MYERS, RYAN LOZAR, TERESA J. MCGARRY, CHARLENE OLIVER, TORALF PETERS, MARIO SAMPEDRO, TIMOTHY SEBERT, ZACHARY SHARPER, ROBERT SLATER, DARREN STRICKLAND, PETER ULIANO, NANCY WHEATLEY, KIMBERLY WINSOR (Attachments: # 1 Exhibit A)(Girard, Daniel) (Entered: 08/01/2017)
08/01/2017		MINUTE ORDER. The Court has the motions to dismiss in this multidistrict litigation under advisement and is aware of the decision issued by the D.C. Circuit Court of Appeals in Attias v. CareFirst, Inc., case no. 16−7108. Given this, counsel need not file a notice of additional authority, but either side may address the application of the opinion to the issues pending before this Court in a submission no longer that five pages filed by August 15, 2017. Any submissions should not repeat arguments or authorities set forth previously. Signed by Judge Amy Berman Jackson on 8/1/17. (DMK) (Entered: 08/01/2017)
08/04/2017	112	SUPPLEMENTAL MEMORANDUM to re 81 MOTION to Dismiss *NTEU Plaintiffs' Amended Complaint* filed by EUGENE GAMBARDELLA, STEPHEN HOWELL, NATIONAL TREASURY EMPLOYEES UNION, JOHN ORTINO. (Shah, Paras) (Entered: 08/04/2017)

08/15/2017	113	SUPPLEMENTAL MEMORANDUM re 72 MOTION to Dismiss *the Consolidated Amended Complaint* filed by KATHERINE ARCHULETA, 81 MOTION to Dismiss *NTEU Plaintiffs' Amended Complaint* filed by BETH F. COBERT by UNITED STATES OFFICE OF PERSONNEL MANAGEMENT. (Carmichael, Andrew) Modified event title on 8/16/2017 (znmw). (Entered: 08/15/2017)
08/15/2017	114	SUPPLEMENTAL MEMORANDUM re 70 MOTION to Dismiss filed by KEYPOINT GOVERNMENT SOLUTIONS by KEYPOINT GOVERNMENT SOLUTIONS. (Mendro, Jason) Modified event title on 8/16/2017 (znmw). (Entered: 08/15/2017)
08/15/2017	115	SUPPLEMENTAL MEMORANDUM re 82 Memorandum in Opposition,,, filed by JOHNNY GONZALEZ, PAUL DALY, MICHAEL EBERT, AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL−CIO, KIMBERLY WINSOR, PETER ULIANO, JOHN DOE III, ZACHARY SHARPER, RYAN LOZAR, JOHN DOE, ROBERT SLATER, CHARLENE OLIVER, TONY BACHTELL, MONTY BOS, JANE DOE, MICHAEL HANAGAN, TIMOTHY SEBERT, TRAVIS ARNOLD, TERESA J. MCGARRY, MICHAEL JOHNSON, MARYANN HIBBS, TORALF PETERS, ROBERT CRAWFORD, CYNTHIA KING−MYERS, HEATHER BURNETT−RICK, MYRNA BROWN, DARREN STRICKLAND, JENNIFER GUM, GARDELL BRANCH, JANE DOE II, DEBORAH HOFFMAN, NANCY WHEATLEY, RYAN BONNER, KELLY FLYNN, ALIA FULI, ORIN GRIFFITH, MARIO SAMPEDRO, LILLIAN GONZALEZ−COLON, JOHN DOE II by AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL−CIO, TRAVIS ARNOLD, TONY BACHTELL, RYAN BONNER, MONTY BOS, GARDELL BRANCH, MYRNA BROWN, HEATHER BURNETT−RICK, ROBERT CRAWFORD, PAUL DALY, JANE DOE, JOHN DOE, JANE DOE II, JOHN DOE II, JOHN DOE III, MICHAEL EBERT, KELLY FLYNN, ALIA FULI, JOHNNY GONZALEZ, LILLIAN GONZALEZ−COLON, ORIN GRIFFITH, JENNIFER GUM, MICHAEL HANAGAN, MARYANN HIBBS, DEBORAH HOFFMAN, MICHAEL JOHNSON, CYNTHIA KING−MYERS, RYAN LOZAR, TERESA J. MCGARRY, CHARLENE OLIVER, TORALF PETERS, MARIO SAMPEDRO, TIMOTHY SEBERT, ZACHARY SHARPER, ROBERT SLATER, DARREN STRICKLAND, PETER ULIANO, NANCY WHEATLEY, KIMBERLY WINSOR. (Girard, Daniel) Modified event title on 8/16/2017 (znmw). (Entered: 08/15/2017)
09/19/2017	116	ORDER granting 70 Defendant KeyPoint Government Solutions, Inc.'s Motion to Dismiss Plaintiffs' Consolidated Amended Complaint; granting 72 Federal Defendant's Motion to Dismiss the Consolidated Amended Complaint; and granting 81 Federal Defendant's Motion to Dismiss the NTEU Plaintiffs' Amended Complaint. See Order for details. Signed by Judge Amy Berman Jackson on 9/19/17. (DMK) (Entered: 09/19/2017)
09/19/2017	117	MEMORANDUM OPINION. Signed by Judge Amy Berman Jackson on 9/19/17. (DMK) (Entered: 09/19/2017)
09/19/2017	118	NOTICE OF APPEAL TO DC CIRCUIT COURT as to 116 Order on Motion to Dismiss,,,,, 117 Memorandum & Opinion by EUGENE GAMBARDELLA, STEPHEN HOWELL, NATIONAL TREASURY EMPLOYEES UNION, JOHN ORTINO. Filing fee $ 505, receipt number 0090−5122668. Fee Status: Fee Paid. Parties have been notified. (Shah, Paras) (Entered: 09/19/2017)
09/20/2017	119	Transmission of the Notice of Appeal, Order Appealed (Memorandum Opinion), and Docket Sheet to US Court of Appeals. The Court of Appeals fee was paid this date re 118 Notice of Appeal to DC Circuit Court. (znmw) (Entered: 09/20/2017)
09/27/2017		USCA Case Number 17−5217 for 118 Notice of Appeal to DC Circuit Court, filed by NATIONAL TREASURY EMPLOYEES UNION, JOHN ORTINO, STEPHEN HOWELL, EUGENE GAMBARDELLA. (zrdj) (Entered: 09/28/2017)
10/05/2017	120	NOTICE OF APPEAL TO DC CIRCUIT COURT as to 116 Order on Motion to Dismiss,,,,, 117 Memorandum & Opinion by AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL−CIO, TRAVIS ARNOLD, TONY BACHTELL, RYAN BONNER, MONTY BOS, GARDELL BRANCH, MYRNA BROWN, HEATHER BURNETT−RICK, ROBERT CRAWFORD, PAUL DALY, JANE DOE, JOHN DOE, JANE DOE II, JOHN DOE II, JOHN DOE III, MICHAEL

		EBERT, KELLY FLYNN, ALIA FULI, JOHNNY GONZALEZ, LILLIAN GONZALEZ−COLON, ORIN GRIFFITH, JENNIFER GUM, MICHAEL HANAGAN, MARYANN HIBBS, DEBORAH HOFFMAN, MICHAEL JOHNSON, CYNTHIA KING−MYERS, RYAN LOZAR, TERESA J. MCGARRY, CHARLENE OLIVER, TORALF PETERS, MARIO SAMPEDRO, TIMOTHY SEBERT, ZACHARY SHARPER, ROBERT SLATER, DARREN STRICKLAND, PETER ULIANO, NANCY WHEATLEY, KIMBERLY WINSOR. Filing fee $ 505, receipt number 0090−5147740. Fee Status: Fee Paid. Parties have been notified. (Girard, Daniel) (Entered: 10/05/2017)
10/06/2017	121	Transmission of the Notice of Appeal, Order Appealed (Memorandum Opinion), and Docket Sheet to US Court of Appeals. The Court of Appeals fee was paid this date re 120 Notice of Appeal to DC Circuit Court. (znmw) (Entered: 10/06/2017)
10/11/2017	122	Amended NOTICE OF APPEAL re appeal 120 by AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL−CIO, TRAVIS ARNOLD, TONY BACHTELL, RYAN BONNER, MONTY BOS, GARDELL BRANCH, MYRNA BROWN, HEATHER BURNETT−RICK, ROBERT CRAWFORD, PAUL DALY, JANE DOE, JOHN DOE, JANE DOE II, JOHN DOE II, JOHN DOE III, MICHAEL EBERT, KELLY FLYNN, ALIA FULI, JOHNNY GONZALEZ, LILLIAN GONZALEZ−COLON, ORIN GRIFFITH, JENNIFER GUM, MICHAEL HANAGAN, MARYANN HIBBS, DEBORAH HOFFMAN, CYNTHIA KING−MYERS, RYAN LOZAR, TERESA J. MCGARRY, CHARLENE OLIVER, TORALF PETERS, MARIO SAMPEDRO, TIMOTHY SEBERT, ZACHARY SHARPER, ROBERT SLATER, DARREN STRICKLAND, PETER ULIANO, NANCY WHEATLEY, KIMBERLY WINSOR. (Girard, Daniel) (Entered: 10/11/2017)
10/12/2017	123	Supplemental Record on Appeal transmitted to US Court of Appeals re 122 Amended Notice of Appeal; USCA Case Number: Unknown. (znmw) (Entered: 10/12/2017)
10/12/2017		USCA Case Number 17−5232 for 122 Amended Notice of Appeal,, filed by JOHNNY GONZALEZ, PAUL DALY, MICHAEL EBERT, AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL−CIO, KIMBERLY WINSOR, PETER ULIANO, JOHN DOE III, ZACHARY SHARPER, RYAN LOZAR, JOHN DOE, ROBERT SLATER, CHARLENE OLIVER, TONY BACHTELL, MONTY BOS, JANE DOE, MICHAEL HANAGAN, TIMOTHY SEBERT, TRAVIS ARNOLD, TERESA J. MCGARRY, MARYANN HIBBS, TORALF PETERS, ROBERT CRAWFORD, CYNTHIA KING−MYERS, HEATHER BURNETT−RICK, MYRNA BROWN, DARREN STRICKLAND, JENNIFER GUM, GARDELL BRANCH, JANE DOE II, DEBORAH HOFFMAN, NANCY WHEATLEY, RYAN BONNER, KELLY FLYNN, ALIA FULI, ORIN GRIFFITH, MARIO SAMPEDRO, LILLIAN GONZALEZ−COLON, JOHN DOE II, 118 Notice of Appeal to DC Circuit Court, filed by NATIONAL TREASURY EMPLOYEES UNION, STEPHEN HOWELL, JOHN ORTINO, EUGENE GAMBARDELLA. (zrdj) (Entered: 10/12/2017)
11/07/2017	124	NOTICE of Change of Address by Tina Wolfson (Wolfson, Tina) (Entered: 11/07/2017)
11/08/2017	125	NOTICE OF APPEAL TO THE FEDERAL CIRCUIT as to 116 Order on Motion to Dismiss,,,,, 117 Memorandum & Opinion by AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL−CIO, TRAVIS ARNOLD, TONY BACHTELL, RYAN BONNER, MONTY BOS, GARDELL BRANCH, MYRNA BROWN, HEATHER BURNETT−RICK, ROBERT CRAWFORD, PAUL DALY, JANE DOE, JOHN DOE, JANE DOE II, JOHN DOE II, JOHN DOE III, MICHAEL EBERT, KELLY FLYNN, ALIA FULI, JOHNNY GONZALEZ, LILLIAN GONZALEZ−COLON, ORIN GRIFFITH, JENNIFER GUM, MICHAEL HANAGAN, MARYANN HIBBS, DEBORAH HOFFMAN, MICHAEL JOHNSON, CYNTHIA KING−MYERS, RYAN LOZAR, TERESA J. MCGARRY, CHARLENE OLIVER, TORALF PETERS, MARIO SAMPEDRO, TIMOTHY SEBERT, ZACHARY SHARPER, ROBERT SLATER, DARREN STRICKLAND, PETER ULIANO, NANCY WHEATLEY, KIMBERLY WINSOR. Filing fee $ 505, receipt number 0090−5197882. Fee Status: Fee Paid. Parties have been notified. (Girard, Daniel) (Entered: 11/08/2017)

11/09/2017	126	ENTERED IN ERROR.....Transmission of the Notice of Appeal, Order Appealed (Memorandum Opinion), and Docket Sheet to US Court of Appeals. The Court of Appeals fee was paid this date re 125 Notice of Appeal to the Federal Circuit. (znmw) Modified on 11/9/2017 (znmw). (Entered: 11/09/2017)
11/09/2017		NOTICE OF CORRECTED DOCKET ENTRY: Docket Entry 126 Transmission of Notice of Appeal and Docket Sheet to USCA was entered in error and will be retransmitted to the Federal Circuit. (znmw) (Entered: 11/09/2017)
11/09/2017	127	Transmission of the Notice of Appeal, Order Appealed (Memorandum Opinion), and Docket Sheet to Federal Circuit. The appeal fee was paid this date re 125 Notice of Appeal to the Federal Circuit. (znmw) (Entered: 11/09/2017)
11/15/2017		USCA Federal Circuit Case Number 18−1182−CB for 125 Notice of Appeal to the Federal Circuit filed by JOHNNY GONZALEZ, PAUL DALY, MICHAEL EBERT, AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL−CIO, KIMBERLY WINSOR, PETER ULIANO, JOHN DOE III, ZACHARY SHARPER, RYAN LOZAR, JOHN DOE, ROBERT SLATER, CHARLENE OLIVER, TONY BACHTELL, MONTY BOS, JANE DOE, MICHAEL HANAGAN, TIMOTHY SEBERT, TRAVIS ARNOLD, TERESA J. MCGARRY, MICHAEL JOHNSON, MARYANN HIBBS, TORALF PETERS, ROBERT CRAWFORD, CYNTHIA KING−MYERS, HEATHER BURNETT−RICK, MYRNA BROWN, DARREN STRICKLAND, JENNIFER GUM, GARDELL BRANCH, JANE DOE II, DEBORAH HOFFMAN, NANCY WHEATLEY, RYAN BONNER, KELLY FLYNN, ALIA FULI, ORIN GRIFFITH, MARIO SAMPEDRO, LILLIAN GONZALEZ−COLON, JOHN DOE II. (zrdj) (Entered: 12/01/2017)
11/21/2017	128	NOTICE of Transcript Purchase Order Form re 125 Notice of Appeal to the Federal Circuit (zrdj) (Entered: 12/04/2017)
12/18/2017	129	ORDER of USCA Federal Circuit as to 125 Notice of Appeal to the Federal Circuit, filed by JOHNNY GONZALEZ, PAUL DALY, MICHAEL EBERT, AMERICAN FEDERATION OF GOVERNMENT EMPLOYEES, AFL−CIO, KIMBERLY WINSOR, PETER ULIANO, JOHN DOE III, ZACHARY SHARPER, RYAN LOZAR, JOHN DOE, ROBERT SLATER, CHARLENE OLIVER, TONY BACHTELL, MONTY BOS, JANE DOE, MICHAEL HANAGAN, TIMOTHY SEBERT, TRAVIS ARNOLD, TERESA J. MCGARRY, MICHAEL JOHNSON, MARYANN HIBBS, TORALF PETERS, ROBERT CRAWFORD, CYNTHIA KING−MYERS, HEATHER BURNETT−RICK, MYRNA BROWN, DARREN STRICKLAND, JENNIFER GUM, GARDELL BRANCH, JANE DOE II, DEBORAH HOFFMAN, NANCY WHEATLEY, RYAN BONNER, KELLY FLYNN, ALIA FULI, ORIN GRIFFITH, MARIO SAMPEDRO, LILLIAN GONZALEZ−COLON, JOHN DOE II ; USCA Federal Circuit Case Number 18−1182−CB. (zrdj) (Entered: 01/03/2018)

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN RE: U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION	Misc. Action No. 15-1394 (ABJ) MDL Docket No. 2664
This Document Relates To: ALL CASES	

CONSOLIDATED AMENDED COMPLAINT

I. NATURE OF THE ACTION

1. This action arises from the failure of Defendants the United States Office of Personnel Management ("OPM") and its security contractor KeyPoint Government Solutions, Inc. ("KeyPoint"), to establish legally required safeguards to ensure the security of government investigation information of current, former, and prospective employees of the federal government and its contractors. Defendants' failure to implement adequate, compulsory security measures in the face of known, ongoing, and persistent cyber threats—and despite repeated warnings of their systems' vulnerabilities—resulted in data breaches affecting more than 21 million people. The government investigation information ("GII") exposed and stolen in these breaches is private and sensitive, consisting of fingerprint records, detailed personal, financial, medical, and associational histories, Social Security numbers and birthdates of employees and their family members, and other private facts collected in federal background and security clearance investigations and stored on Defendants' electronic systems.

2. OPM announced a series of data breaches in 2015. For years before the announcement, OPM officials knew that OPM's systems lacked critical security safeguards and controls. Since 2007, audits carried out by the Office of Inspector General ("IG"), an independent office within OPM, warned that OPM's information security systems, management, and protocols were inordinately lax and vulnerable to electronic incursions. The OPM Inspector General's audits determined that OPM lacked not only the technology and oversight to protect its systems from cyberattacks but also the ability to discern the existence and extent of such an attack. OPM failed to remedy these known deficiencies and failed to follow its auditors' guidance for bringing its cybersecurity defenses into compliance with federal requirements.

3. OPM officials knew that OPM was a prime target for cyberattacks. OPM officials were aware of constant hacking attempts against OPM's systems. OPM's systems were breached in 2009 and 2012. A November 2013 attack compromised critical security documents.

4. Then in about December 2013, an unknown person or persons obtained the user log-in credentials of a KeyPoint employee. Those credentials were used to invade KeyPoint's systems and steal the personnel records of tens of thousands of Department of Homeland Security employees (the "KeyPoint Breach").

5. OPM learned in September 2014 of the December 2013 cyberattack on KeyPoint. OPM did not terminate or suspend its contract with KeyPoint, limit KeyPoint's access to OPM's systems, or take remedial actions necessary to protect OPM's systems from incursions made possible by the KeyPoint Breach.

6. Hackers used KeyPoint credentials to breach OPM's information systems in May 2014 and maintained access to OPM's information systems for over a year. Once inside OPM's network, the hackers gained access to another set of OPM servers stored in the Interior

Department. The attacks begun in 2014 (the "OPM Breaches") went undetected for several months. By the time they were discovered, vast amounts of sensitive information had been extracted from OPM's network.

7. The victims of the KeyPoint Breach and the OPM Breaches (together, the "Data Breaches") have sustained economic harm from misuse of the stolen information, and their GII remains subject to a continuing risk of additional exposure or theft as a consequence of OPM's ongoing failure to secure it.

8. The IG issued its most recent audit of OPM's electronic systems in November 2015. The audit determined that most of the vulnerabilities exploited in the OPM Breaches still exist and, in some instances, have worsened. As in 2014, the IG advised OPM to shut down several of its major systems that are operating without security authorizations in violation of law. As in 2014, OPM has refused to do so, on the basis that accessibility of data to assist its continuing operations takes precedence over securing the confidentiality and integrity of the GII under its control.

9. Defendants' failure to protect GII, despite repeated official warnings of cyber threats and security lapses in their systems, constitutes willful misconduct. OPM, unlawfully prioritizing convenience over safety and ignoring direction from its federal auditors, violated the Privacy Act, the Federal Information Security Management Act, the Federal Information Security Modernization Act, and the Administrative Procedure Act and breached its contracts with Plaintiffs and Class members. KeyPoint's actions and inactions constitute negligence, negligent misrepresentation and concealment, invasion of privacy, breach of contract, and violations of the Fair Credit Reporting Act and state statutes.

II. PARTIES

A. Plaintiffs

10. Plaintiffs bring this action on behalf of individuals whose sensitive personal information was compromised in the OPM Breaches or in the KeyPoint Breach. As used herein, "sensitive personal information" includes, at a minimum, Social Security numbers and birthdates, but may also include the range of GII compromised in the Data Breaches.

11. Plaintiff American Federation of Government Employees ("AFGE") is a labor organization headquartered at 80 F Street, N.W., Washington, D.C. 20001. AFGE represents, on its own and through its affiliated councils and locals, approximately 650,000 civilian employees in departments and agencies throughout the federal government, for a variety of purposes. AFGE conducts collective bargaining on behalf of employees it represents, and it works to ensure that its members' rights, including statutory and contractual rights, are honored and protected by their employers. Workers in virtually all domains of the federal government depend on AFGE for legal representation, legislative advocacy, technical expertise, and informational services.

12. In this action, AFGE seeks declaratory and injunctive relief only on behalf of the Class. OPM has notified hundreds of thousands of AFGE members that their GII was compromised in the OPM Breaches. AFGE has actively pursued and defended its members' rights and interests relating to this controversy, including by requesting that they be afforded administrative leave to register for identity theft protection services and to manage any other fallout from the OPM Breaches, and by seeking lifetime identify theft protection services for all federal employees.

13. Plaintiff Travis Arnold resides and is domiciled in the state of Arizona. He formerly served in Field Artillery at the Department of Defense for approximately twelve years. Arnold provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. In May 2015, while reviewing his bank statement, Arnold discovered an unauthorized charge of approximately $125 for a purchase in China. He has spent approximately ten hours communicating with employees of his bank to reverse this fraudulent transaction and submitting documents detailing the fraud. While reviewing his credit report, Arnold also learned that between six and ten inquiries regarding his credit had been made by companies with which he had no prior relationship. Arnold has spent many hours disputing these fraudulent inquiries. He suffers stress related to concerns for his personal safety and that of his family members. His exposure to the Data Breaches has also caused Arnold to review his credit reports and financial accounts with greater frequency.

14. Plaintiff Tony Bachtell resides and is domiciled in the state of Wisconsin. He currently works as a floor covering specialist at Orion Hardwood Floors, a federal government contractor. Bachtell provided sensitive personal information to the federal government. He and his wife received notice from OPM that such information has been compromised in the Data Breaches. In February 2016, the Internal Revenue Service informed Bachtell that a fraudulent tax return for the 2015 tax year had been filed using his and his wife's personal information. Bachtell has spent many hours attempting to resolve this tax fraud issue. Payment of his tax refunds will be delayed for several months. Also in February 2016, the Social Security Administration informed Bachtell that an unknown individual had used his and his wife's personal information to create online "My Social Security" accounts. Such accounts can be used

to request a replacement Social Security card and to obtain estimates of a Social Security cardholder's future retirement benefits and the amount he or she has paid in Social Security and Medicare taxes. Thereafter, Bachtell learned that approximately ten inquiries regarding his credit had been made by companies with which he had no prior relationship. Bachtell has devoted many hours to remedial actions, including placing a freeze on his credit and communicating with the Social Security Administration to terminate the unauthorized accounts. His exposure to the Data Breaches has also caused Bachtell to review his credit reports and financial accounts with greater frequency.

15. Plaintiff Ryan Bonner resides and is domiciled in the state of Pennsylvania. He formerly worked at the Transportation Security Administration, as a Transportation Security Officer. Bonner provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. His exposure to the Data Breaches has caused Bonner to review his credit reports and financial accounts with greater frequency.

16. Plaintiff Monty Bos resides and is domiciled in the state of Oklahoma. He currently works as a Processor with ASRC Federal Primus, a federal government contractor. Bos previously worked as a Tractor Operator for the Army's Directorate of Plans, Training, Mobilization, and Security. Bos provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Bos thereafter learned that an unauthorized credit card account had been opened in his name. He now reviews his credit reports every month to detect fraudulent activity.

17. Plaintiff Gardell Branch resides and is domiciled in the state of Illinois. He formerly worked as a Casual Mail Handler at the Postal Service. Branch provided sensitive personal information to the federal government, including in an SF-85 form, and received notice from OPM that such information has been compromised in the Data Breaches. Branch thereafter purchased monthly credit monitoring services from Equifax. Additionally, the Social Security Administration notified Branch that an unknown individual had attempted to use his Social Security Number. This incident required Branch to spend time verifying his identity and creating an identity theft profile with the Social Security Administration. His exposure to the Data Breaches has also caused Branch to review his financial accounts with greater frequency. He now reviews his bank and credit card accounts at least every other day to detect fraudulent activity.

18. Plaintiff Myrna Brown resides and is domiciled in the state of New Mexico. She formerly worked as an International Trade Specialist in the Foreign Commercial Service of the Commerce Department. Brown provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Her exposure to the Data Breaches has caused Brown to review her financial accounts with greater frequency. Brown now also reviews her credit reports regularly to detect fraudulent activity. Additionally, Brown suffers stress resulting from fear that the theft of her sensitive personal information will impair her ability to obtain future federal government employment or security clearances, and fear for the safety of her family members who serve in the military.

19. Plaintiff Heather Burnett-Rick resides and is domiciled in the state of Michigan. She currently works as a Foreman with the Federal Bureau of Prisons, and formerly

served in the National Guard for approximately twelve years. Additionally, Burnett-Rick applied to be a Border Patrol Agent with Customs and Border Protection and an Air Marshal with the Federal Air Marshal Service. She and her husband provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. CSIdentity Corporation ("CSID") thereafter informed Burnett-Rick that her work email address had been found on the "dark web." The dark web consists of parts of the World Wide Web that cannot be accessed with standard web technology or located with ordinary search engines or browsers and which use encryption to conceal the identity of those operating the websites. Dark websites are predominantly used to facilitate illicit activities, such as drug trafficking and identity theft. Burnett-Rick also learned from her bank that her debit card number had been used in an unauthorized attempt to make charges in Indiana of approximately $900, and that additional unauthorized charges of approximately $300 had been approved and deducted from her checking account. She spent about ten hours speaking with employees of her bank and reviewing and submitting affidavits and other documents to dispute these unauthorized charges. Burnett-Rick suffers stress resulting from concerns that her exposure to the Data Breaches will adversely affect her minor children's future and concerns that her fingerprints and sensitive personal information will be used to commit identity theft. Her exposure to the Data Breaches has also caused Burnett-Rick to review her financial accounts with greater frequency.

20. Plaintiff Robert Crawford resides and is domiciled in the state of Indiana. He currently works as an Operating Practices Inspector with the Federal Railroad Administration, and previously served in the Navy for approximately 29 years. Crawford provided sensitive personal information to the federal government and received notice from OPM that such

information has been compromised in the Data Breaches. Thereafter, Crawford placed fraud alerts on his credit and began reviewing his credit reports and financial statements every day.

21. Plaintiff Paul Daly resides and is domiciled in the state of Florida. He formerly worked as a Manager of Distribution Operations at the Postal Service, where he was employed for approximately 37 years. Daly's wife formerly worked at the Internal Revenue Service. Daly and his wife provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In April 2015, the Internal Revenue Service informed Daly that fraudulent tax returns for the 2014 tax year had been filed using his and his wife's personal information (on separate tax return forms). Daly has spent many hours attempting to resolve these tax fraud issues, which remain under investigation by the Internal Revenue Service. Additionally, he closed financial accounts and opened new ones, and purchased credit monitoring services through Equifax, for which he pays $29.95 per month. His exposure to the Data Breaches has also caused Daly to review his financial accounts with greater frequency, and to refrain from online bill payment activities, which has caused him to incur $30.95 per month in fees to make payments over the phone for his wife's car and for their credit card and phone bills.

22. Plaintiff Jane Doe currently resides in Virginia and plans to relocate to Kentucky in May 2016 due to her husband's military transfer orders. She is using the pseudonym "Jane Doe" in this action because of her personal safety concerns. Doe currently works as an Information Technology Specialist Project Manager at the Department of Housing and Urban Development. She formerly worked at various federal agencies in positions that similarly involved monitoring and controlling computer systems. Doe's husband serves in the Army. Doe and her husband each provided sensitive personal information to the federal government,

including in SF-86 forms. Doe and her husband each received notice from OPM that such information has been compromised in the Data Breaches. In August 2015, the Federal Bureau of Investigation informed Doe that her GII had been acquired by the so-called Islamic State of Iraq and al-Sham ("ISIS"). While reviewing her credit report, Doe discovered that twelve unknown accounts had been fraudulently opened in her name and were in collections. She paid approximately $198 to a credit repair law firm for assistance in closing the fraudulent accounts and removing them from her credit report. As of this filing, only some of these fraudulent accounts have been closed. When Doe attempted to access her credit report online with TransUnion, she found that she was unable to do so because TransUnion could not verify her identity. Doe has spent between 40 and 50 hours dealing with the fraudulent accounts, communicating with the FBI, and attempting to gain access to her credit report with TransUnion. She expended approximately $50 to obtain copies of her credit report. Doe suffers stress resulting from concerns for her personal safety and that of her family members, and concerns that her exposure to the Data Breaches will impair her ability to obtain a job transfer and the Top Secret clearance needed to perform her job. Her exposure to the Data Breaches has also caused Doe to review her credit reports and financial accounts with greater frequency.

23. Plaintiff Jane Doe II resides and is domiciled in the state of Kansas. She is using the pseudonym "Jane Doe II" in this action because of her personal safety concerns. Doe II's spouse is an Assistant United States Attorney responsible for prosecuting large-scale narcotics and money laundering cases, including cases against international drug cartels known to target prosecutors, law enforcement officials, and their families. Doe II's husband has received multiple death threats throughout his career and was the subject of an assassination attempt. Since that attempt, Doe II and her husband have used a P.O. Box miles from their home as their

mailing address, and have maintained unlisted telephone numbers. Doe II and her husband have two minor children. Doe II's husband provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Doe II also received notice from OPM that her sensitive personal information has been compromised in the Data Breaches. Doe II experiences significant stress from fear that the exposure of her and her family members' sensitive personal information will cause them to be targeted for retaliatory attacks and bodily harm. Doe II also experiences stress from concerns that she and her family members face an increased risk of identity theft, fraud, and other types of monetary harm.

24. Plaintiff John Doe resides and is domiciled in the state of Washington. He is using the pseudonym "John Doe" in this action because of his personal safety concerns. He currently works as a Senior Inspector with the Marshals Service, where he has been employed for approximately 27 years. Doe holds a Top Secret clearance and has investigated drug trafficking cartels. Doe provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In February 2016, the Internal Revenue Service informed Doe that a fraudulent tax return for the 2015 tax year had been filed using his and his wife's personal information. Doe has spent five to ten hours attempting to resolve the tax fraud issue. Payment of his tax refunds is expected to be delayed for several months. Doe suffers stress resulting from concerns for his personal safety and that of his family members, and concerns that identity theft will aggravate his health problems and adversely affect his retirement plan.

25. Plaintiff John Doe II resides and is domiciled in the state of Idaho. He is using the pseudonym "John Doe II" in this action because of his personal safety concerns. He

formerly worked for 20 years as a Senior Special Agent with the Customs Service, Office of Enforcement (which merged with Immigration and Naturalization Service, Investigations to form Immigration and Customs Enforcement, a division of the Department of Homeland Security, and was later renamed Homeland Security Investigations). As a member of the Joint Terrorist Task Force, Doe II supervised investigations of terrorism and drug trafficking cartels. His security clearance was above Top Secret, at the Sensitive Compartmented Information level. Doe II provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. He thereafter spent time to change his bank accounts, and he purchased credit monitoring services through LifeLock, for which he pays $329 annually. Doe II suffers stress resulting from concerns for his personal safety and that of his family members. His exposure to the Data Breaches has also caused Doe II to review his credit reports and financial accounts with greater frequency.

26. Plaintiff John Doe III resides and is domiciled in the state of Virginia. He is using the pseudonym "John Doe III" in this action because of his personal safety concerns. Doe III is an independent contractor who works with a federal government contractor. He previously served in the Army. Doe III provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. The Internal Revenue Service thereafter informed Doe III that a fraudulent tax return had been filed using his personal information. Doe III has spent several hours attempting to resolve this tax fraud issue. Payment of his tax refunds will be delayed. His exposure to the Data Breaches has also caused Doe III to review his financial

accounts with greater frequency. He now spends approximately one hour per day reviewing his financial accounts to detect fraudulent activity.

27. Plaintiff Michael Ebert resides and is domiciled in the state of Nevada. Ebert worked for the federal government and its contractors for approximately 45 years. He served for 20 years in the Army. Ebert provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Ebert's wife also received notice from OPM that her sensitive personal information has been compromised in the Data Breaches. His exposure to the Data Breaches has caused Ebert to review his financial accounts with greater frequency. He now reviews his bank and credit card accounts approximately twice per day to detect fraudulent activity.

28. Plaintiff Kelly Flynn resides and is domiciled in the state of Utah. She currently works as a Staff Assistant at the Interior Department's Office of the Solicitor. She formerly worked at the Air Force, the Navy, the Internal Revenue Service, and the Postal Service. Flynn provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In spring 2015, the Internal Revenue Service informed Flynn that a fraudulent tax return for the 2014 tax year had been filed using her and her husband's personal information. The investigation into this tax fraud issue remains pending. As a result, Flynn has not yet received her federal or state income tax refunds for the 2014 tax year. In July 2015, after learning of the Data Breaches, Flynn added credit monitoring from the three major credit bureaus, at a cost of $10 per month, to her preexisting credit and identity monitoring services. Flynn thereafter learned that a Barclays Bank credit card and a JCPenney credit card had been fraudulently opened in her name. Flynn's

husband also learned that two credit card accounts had been fraudulently opened in his name. Additionally, Equifax notified Flynn that a $5,000 loan from Cash Central had been taken out in her name online, and that the loan was delinquent and in collections. On March 1, 2016, Flynn's husband learned that a loan of over $1,400 with Castle Creek Payday Loans had been taken out in his name online, and was delinquent. Flynn has spent over 50 hours attempting to resolve the tax fraud issues and to close the fraudulent accounts and terminate the fraudulent loans. Her exposure to the Data Breaches has also caused Flynn to review her credit reports and financial accounts with greater frequency. Flynn suffers stress resulting from concerns that her and her family members' identities will be stolen.

29. Plaintiff Alia Fuli resides and is domiciled in the state of Nevada. She currently works as a Service Representative at the Social Security Administration, and formerly worked as a Medical Reimbursement Technician and Patient Accounts Representative at the Department of Veterans Affairs. Fuli began working for the Department of Veterans Affairs in 2011. Fuli provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In December 2015, Fuli learned that a PayPal/Synchrony Bank credit card account had been opened in her name and used to make unauthorized online purchases of approximately $298. Fuli has spent approximately 15 hours communicating with PayPal representatives in an attempt to get these charges reversed and the fraudulent account closed. While reviewing her credit report, Fuli also learned that between July 2015 and December 2015, multiple inquiries regarding her credit had been made by companies with which she had no prior relationship. Her exposure to the Data Breaches has caused Fuli to review her credit reports and financial accounts with greater frequency.

30. Plaintiff Johnny Gonzalez resides and is domiciled in the state of Florida. He currently works as a Deportation Officer at Immigrations and Customs Enforcement, and formerly worked as a Border Patrol Agent at Customs and Border Protection. Gonzalez provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Gonzalez's bank thereafter informed him that his debit card number had been used to make unauthorized charges of approximately $360 in China. In January 2016, Gonzalez's bank informed him that an unauthorized attempt had been made to charge approximately $1,000 on his debit card number in Florida, and that an additional $96 in unauthorized charges had been approved and deducted from his checking account. In late 2015, Gonzalez also learned that his credit card number had been used to make an unauthorized charge of approximately $100 in Massachusetts. Gonzalez has spent approximately 20 hours attempting to reverse the fraudulent financial transactions and closing his checking account with his bank and opening a new account. Gonzalez suffers stress resulting from concerns that his exposure to the Data Breaches will impair his ability to renew his current security clearance and/or to obtain a higher security clearance in the future. His exposure to the Data Breaches has also caused Gonzalez to review his financial accounts with greater frequency.

31. Plaintiff Lillian Gonzalez-Colon resides and is domiciled in the state of Florida. She currently works as a Medical Technologist at the Department of Veterans Affairs. She began working for the Department of Veterans Affairs in 2012. Gonzalez-Colon provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In December 2014, Gonzalez-Colon learned that a series of inquiries regarding her credit had been made in connection with an

unauthorized attempt to open fraudulent accounts in her name. In January 2015, the Internal Revenue Service informed Gonzalez-Colon that an unknown individual had fraudulently claimed her 4-year-old son as a dependent on a tax return filed in New York for the 2014 tax year. As a result, payment of her tax refunds was delayed for three months. In February 2016, Gonzalez-Colon's mortgage lenders informed her that an account with Verizon Wireless had been opened in her name in December 2014 and that this account had an outstanding balance of almost $3,000. The fraudulent account remains under investigation by Verizon Wireless. Gonzalez-Colon has spent over 100 hours in attempts to resolve the fraudulent tax return filing and to close the fraudulent Verizon Wireless account. These efforts required her to take time off work. Her exposure to the Data Breaches has caused Gonzalez-Colon to review her credit reports and financial accounts with greater frequency. Gonzalez-Colon suffers stress resulting from concerns that her exposure to the Data Breaches will adversely affect her minor children's future.

32. Plaintiff Orin Griffith resides and is domiciled in the state of Oklahoma. Griffith currently serves as an Aircraft Mechanic in the Air Force, and formerly served as an Aircraft Weapons Mechanic in the Army. Griffith provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. In February 2015, the Internal Revenue Service informed Griffith that a fraudulent tax return for the 2014 tax year had been filed using his and his wife's personal information. Griffith has spent several hours attempting to resolve this tax fraud issue. Payment of his tax refunds was delayed for almost ten months. Griffith's exposure to the Data Breaches has caused him to review his financial accounts with greater frequency.

33. Plaintiff Jennifer Gum resides and is domiciled in the state of Kansas. She works as a Medical Reimbursement Technician for the Veterans Affairs Medical Center, and her

husband works as a Senior Corrections Officer with the Federal Bureau of Prisons. She began working for the Department of Veterans Affairs in 2011. Gum and her husband provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. Her exposure to the Data Breaches has caused Gum to review her financial accounts with greater frequency.

34. Plaintiff Michael Hanagan resides and is domiciled in the state of California. He currently works as a Capital Habeas Staff Attorney in the United States District Court for the Central District of California. Hanagan provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Hanagan thereafter purchased a monthly subscription for credit and identity monitoring and purchased copies of his credit reports to detect fraudulent activity.

35. Plaintiff Maryann Hibbs resides and is domiciled in the state of Pennsylvania. She currently works as a Registered Nurse at the Veterans Health Administration, where she has been employed for approximately 23 years. Hibbs also previously served in the Army National Guard. Hibbs provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. Hibbs suffers stress resulting from concerns for her personal safety and that of her family members.

36. Plaintiff Deborah Hoffman resides and is domiciled in the state of Texas. She currently works as a transcriptionist with Datagain, a federal government contractor. Hoffman provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Her exposure to the Data Breaches has caused Hoffman to review her financial

accounts with greater frequency. She now checks her bank and credit card accounts daily to detect fraudulent activity.

37. Plaintiff Michael Johnson resides and is domiciled in the state of Washington. He currently works as a project director for Camo2Commerce, a federal government contractor. Johnson previously worked in military and federal government positions for over 30 years. He was Chief of Operations for the Multi-National Force in Iraq, a Military Police Officer in the Air Force, and a Platoon Leader in the Army. Johnson also worked as an investigator for KeyPoint. Johnson provided sensitive personal information to the federal government, including in an SF-86 form. He and his wife separately received notice from OPM that such information has been compromised in the Data Breaches. As a retired Senior Army Officer and former Chief of Operations in Iraq, Johnson experiences significant stress from fear that the exposure of his and his family's sensitive personal information will cause him and his family to be targeted for retaliatory attacks and bodily harm. His exposure to the Data Breaches has also caused him to review his financial accounts with greater frequency.

38. Plaintiff Cynthia King-Myers resides and is domiciled in the state of Illinois. She is currently employed as a Social Worker at the Department of Veterans Affairs. She began working for the Department of Veterans Affairs in 2013. King-Myers provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In May 2015, King-Myers learned that unauthorized charges of approximately $658 had been incurred on her debit card account. King-Myers has spent between 30 and 35 hours attempting to reverse these fraudulent transactions. Her exposure to the Data Breaches has also caused King-Myers to review her credit reports and financial accounts with greater frequency.

39. Plaintiff Ryan Lozar resides and is domiciled in the state of New York. He formerly worked as a Law Clerk in the United States District Court for the Eastern District of New York, a Law Clerk in the United States District Court for the District of Puerto Rico, and a Special Assistant United States Attorney in the United States Attorney's Office for the Southern District of California. Lozar provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Lozar thereafter learned that an unknown individual had opened a PayPal account in his name and received a $1,000 cash advance. He also learned that an unknown individual had opened a Best Buy account in his name and used it to purchase $3,500 worth of merchandise. Lozar spent many hours communicating with PayPal and Best Buy to dispute and resolve these fraudulent activities. Lozar then placed a freeze on his credit and contacted the three major credit bureaus to confirm that they were aware of the fraud. Lozar thereafter paid $15 to lift the credit freeze to allow a legitimate inquiry on his credit to be made.

40. Plaintiff Teresa J. McGarry resides and is domiciled in the state of Florida. She currently works in the Social Security Administration as an Administrative Law Judge. McGarry previously served as an Assistant United States Attorney and as a Judge Advocate General with the Navy. McGarry provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. McGarry thereafter purchased a monthly subscription for credit and identity monitoring. Her exposure to the Data Breaches has also caused McGarry to review her financial accounts with greater frequency.

41. Plaintiff Charlene Oliver resides and is domiciled in the state of Mississippi. She formerly served in the Navy, as a Torpedoman's Mate. Oliver's husband formerly served in the

Army, as a Captain of Artillery. Oliver and her husband provided their sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In June 2015, Oliver received a letter from her electricity utility company informing her that her account had been closed, was no longer in her name, and had incurred charges of $500. Oliver also learned that an unknown individual had accessed her electricity account online using her Social Security number and maiden name. Thereafter, her electricity utility company sent her a deposit check for the closed account, but in someone else's name. Oliver has devoted many hours to communicating with her electricity utility company to reverse the fraudulent charges and reopen an account in her name. Her dispute with the company, which claims she must pay another security deposit of $390, is unresolved. Additionally, Oliver learned that fraudulent purchases had been made using her debit card and two credit card numbers. Oliver has spent several hours communicating with her bank and credit card companies to reverse these fraudulent transactions, and she purchased credit monitoring and repair services through a credit repair law firm, for which she pays $100 per month. Her exposure to the Data Breaches has also caused Oliver to review her financial accounts with greater frequency.

42. Plaintiff Toralf Peters resides and is domiciled in the state of Alabama. He is currently a partner of Telesto Group, a subcontractor for the Interior Department and a former subcontractor for the Department of Defense. Peters provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. Among other things, Peters's exposure to the Data Breaches has caused him to review his credit reports and financial accounts with greater frequency. Peters

also suffers stress resulting from concerns that his fingerprints and sensitive personal information will be used to attempt to steal his identity.

43. Plaintiff Mario Sampedro resides and is domiciled in the state of California. He currently works as a Special Agent at the Department of Homeland Security, a position he has held for 26 years. Sampedro provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Sampedro suffers stress resulting from concerns for his personal safety and that of his family members, and concerns regarding the unauthorized use of their sensitive personal information. Sampedro, who is nearing retirement from Homeland Security, worries that the theft of his sensitive personal information will impair his ability to secure future employment with government contractors. His exposure to the Data Breaches has caused Sampedro to review his financial accounts with greater frequency.

44. Plaintiff Timothy Sebert resides and is domiciled in the state of Georgia. Sebert currently works as a Language Analyst for the Navy, where he has served for more than eight years. Sebert and his wife provided sensitive personal information to the federal government, including in SF-86 forms, and received notice from OPM that such information has been compromised in the Data Breaches. Sebert suffers stress resulting from concerns for his personal safety and that of his family members and concerns regarding the unauthorized use of their sensitive personal information. Sebert spent more than five hours reviewing the information in his electronic tax filing account multiple times and changing his account credentials to decrease the chances of his tax refunds being stolen. His exposure to the Data Breaches has also caused Sebert to review his financial accounts with greater frequency.

45. Plaintiff Zachary Sharper resides and is domiciled in the state of Virginia. He currently works as a Contract Specialist Supervisor with the Department of Defense, Defense Logistics Agency. Sharper previously worked as a Corrections Officer at the Bureau of Prisons and a Fuel Systems Operator for the federal government contractor Kellogg Brown & Root. Additionally, Sharper served in the Army for approximately seven years. He provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Sharper thereafter learned accounts had been opened in his name with Sprint and Verizon Wireless, and that six iPhones had been ordered using those accounts. Sharper also received prepaid Green Dot cards he had not ordered. He has spent many hours attempting to resolve these fraudulent transactions.

46. Plaintiff Robert Slater resides and is domiciled in the state of Washington. He currently serves as a Signal Officer, and previously served as a Patriot Missile Operator, in the Army. Slater provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. Slater suffers stress resulting from concerns that the theft of his sensitive personal information will impair his ability to obtain a higher security clearance, or future employment with a government contractor when he leaves the Army. His exposure to the Data Breaches has also caused Slater to review his financial accounts and credit reports with greater frequency to detect fraudulent activity.

47. Plaintiff Darren Strickland resides and is domiciled in the state of North Carolina. Strickland worked for many years for federal government contractors. Strickland provided sensitive personal information to the federal government, including in an SF-86 form, and

received notice from OPM that such information has been compromised in the Data Breaches. His exposure to the Data Breaches has caused Strickland to review his financial accounts with greater frequency.

48. Plaintiff Peter Uliano resides and is domiciled in the state of New Hampshire. He applied for and was offered a position as a Security Screener with the Transportation Security Administration. Uliano provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. Among other things, his exposure to the Data Breaches has caused Uliano to review his financial accounts with greater frequency.

49. Plaintiff Nancy Wheatley resides and is domiciled in the state of Tennessee. She currently works as a registered nurse at the Department of Veterans Affairs. She began working for the Department of Veterans Affairs in 2011, and formerly served in the Army and in the National Guard. Wheatley provided sensitive personal information to the federal government, including in an SF-86 form, and received notice from OPM that such information has been compromised in the Data Breaches. She thereafter learned that unknown individuals had opened fraudulent accounts in her name with Sprint and Virgin Mobile and that unauthorized online purchases had been made using her debit card number. Wheatley has spent many hours attempting to close the fraudulent accounts and to reverse the fraudulent transactions. Her exposure to the Data Breaches has also caused Wheatley to review her financial accounts with greater frequency.

50. Plaintiff Kimberly Winsor resides and is domiciled in the state of Kansas. She is currently employed as a Social Worker at the Department of Veterans Affairs in Kansas City. She began working for the Department of Veterans Affairs in 2015. Winsor and her

husband provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In April 2015, Winsor's husband learned from their bank that his debit card number had been used to make unauthorized purchases in Mississippi. On July 23, 2015, Winsor learned from their bank that her debit card number had been used to make unauthorized purchases in Texas. On November 24, 2015, CSID informed Winsor that her 8-year-old son's Social Security number had been used in California for an unknown purpose. Winsor has spent approximately twelve hours attempting to resolve the fraudulent transactions and the misuse of her son's Social Security number. Among other things, she made trips to her bank to obtain sensitive identifying documents, and completed and submitted affidavits to dispute the fraudulent purchases. Winsor suffers stress resulting from concerns that her exposure to the Data Breaches will adversely affect her minor children's future. Her exposure to the Data Breaches has also caused Winsor to review her financial accounts with greater frequency.

B. Defendants

51. Defendant the United States acted through the Office of Personnel Management.

52. Defendant OPM is a federal agency headquartered at 1900 E Street, N.W., Washington, D.C. 20415. OPM handles many parts of the federal employee recruitment process and, in doing so, collects and maintains federal job applicants' GII, including information provided in background check and security clearance forms. OPM oversees more than two million background checks annually, provides human resources services to other agencies, and audits agency personnel practices.

53. Defendant KeyPoint is a private investigation and security firm incorporated in Delaware. KeyPoint is headquartered and maintains its principal place of business in Loveland,

Colorado. KeyPoint provides fieldwork services for federal background and security clearance checks and employs or contracts with individuals in every state who assist with such investigations.

III. JURISDICTION AND VENUE

54. This Court has subject matter jurisdiction over all the federal claims in this action pursuant to 28 U.S.C. § 1331. The Court also has subject matter jurisdiction over the Privacy Act claim pursuant to 5 U.S.C. § 552a(g)(1)(D) and over the Little Tucker Act claim pursuant to 28 U.S.C. § 1346(a).

55. This Court has subject matter jurisdiction over the claims in this action against KeyPoint pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because Plaintiffs bring class claims on behalf of citizens of states different from KeyPoint's state of citizenship, the total amount in controversy exceeds $5 million, and the proposed Class contains more than 100 members.

56. This Court has personal jurisdiction over OPM because it is headquartered in the District of Columbia and much of the relevant conduct occurred here.

57. This Court has personal jurisdiction over KeyPoint because it conducts significant business in the District of Columbia and much of the relevant conduct occurred here.

58. Venue is proper in this District under 28 U.S.C. § 1391 because OPM is located in the District of Columbia and a substantial part of the events and omissions giving rise to these claims occurred here.

59. Venue is also proper in this District under 5 U.S.C. §§ 552a(g)(5) and 703.

IV. COMMON ALLEGATIONS OF FACT

A. OPM and KeyPoint Collect and Store Confidential Information About Millions of Federal Job Applicants

60. OPM manages the recruitment and retention of the work force of the United States government. As part of its duties, OPM conducts background checks of prospective employees and security clearance checks of current and prospective employees. More than 100 federal agencies depend on OPM's investigatory products and services. OPM oversees more than two million investigations per year, at least 650,000 of which are to support security clearance determinations.

61. As part of its investigatory mandate, OPM collects and stores an enormous amount of information about federal job applicants and past and present federal employees.

62. OPM's Federal Investigative Services division oversees the agency's background and security clearance checks.

63. Federal Investigative Services relies on a software system known as "EPIC." EPIC aggregates and stores information about federal job applicants, including information provided in electronic questionnaires and used in background and security clearance checks. Some of the data in EPIC is sufficiently sensitive that it is housed at the National Security Agency.

64. Among the data stored in EPIC are the master records from investigations of government employees.

65. EPIC also stores the Central Verification System, which contains most background and security clearance check information.

66. The Central Verification System stores versions of Standard Form 86 ("SF-86") as completed by federal job applicants and employees. SF-86 is a 127-page form that every

federal job applicant and employee being considered for a security clearance must fill out and submit.

67. SF-86 contains, among other information, applicants' psychological and emotional health history, police records, illicit drug and alcohol use history, Social Security numbers, birthdates, financial histories and investment records, children's and relatives' names, foreign trips taken and contacts with foreign nationals, past residences, names of neighbors and close friends (such as college roommates and co-workers), and the Social Security numbers and birthdates of spouses, children, and other cohabitants.

68. Each SF-86 form states that the information provided in it "will be protected from unauthorized disclosure." Each SF-86 form also states that the information provided in it "may be disclosed without your consent . . . as permitted by the Privacy Act [5 U.S.C. 552a(b)], and by routine uses." Form SF-86 lists eleven permitted uses.

69. Applicants for non-sensitive federal government or contractor positions must fill out and submit an SF-85 form. Each SF-85 form states that the information provided in it "will be protected from unauthorized disclosure." Each SF-85 form also states that the information provided in it "may be disclosed without your consent . . . as permitted by the Privacy Act [5 U.S.C. 552a(b)], and by routine uses." Form SF-85 lists eleven permitted uses.

70. Applicants for "public trust" federal government or contractor positions must fill out and submit an SF-85P form. Each SF-85P form states that the information provided in it "will be protected from unauthorized disclosure." Each SF-85P form also states that the information provided in it "may be disclosed without your consent . . . as permitted by the Privacy Act [5 U.S.C. 552a(b)], and by routine uses." Form SF-85P lists eleven permitted uses.

71. The Central Verification System stores completed versions of forms SF-85 and SF-85P.

72. The Central Verification System also contains polygraph data, fitness determinations, and decisions made pursuant to Homeland Security Presidential Directive (the background check determinations required for government employees and contractors to gain access to federal facilities).

73. Additionally, the Central Verification System contains detailed information relating to Personal Identification Verification ("PIV") Cards, which are government ID smart cards that government employees and contractors use to access government facilities and software systems.

74. The Electronic Official Personnel Folder is another OPM system that stores personnel files on individual federal employees. The information in such files includes birth certificates, job performance reports, resumes, school transcripts, military service records, employment history and benefits, and job applications that contain Social Security numbers and birthdates.

75. OPM hires contractors to carry out the investigative fieldwork necessary for background and security clearance investigations. KeyPoint performs the majority of OPM's fieldwork. As a contractor of OPM, KeyPoint is subject to the requirements of the Privacy Act to the same extent as OPM. As of June 2015, KeyPoint had received more than $605 million under its OPM contract, with a funding cap of approximately $2.5 billion.

76. To perform its fieldwork, KeyPoint relies on systems that are electronically connected to those of OPM. This linkage allows KeyPoint employees and contractors to download from OPM's network information needed to conduct an investigation, and to upload

investigatory findings to OPM's network. The system through which KeyPoint transmits data to and from OPM's network is called the Secure Portal. The Secure Portal is an electronic conduit through which, among other things, KeyPoint investigators access completed forms and other information stored in OPM's Central Verification System.

77. KeyPoint disseminates its Privacy Policy on the Internet. The policy states that KeyPoint is a consumer reporting agency. The policy further states that KeyPoint is required by the Fair Credit Reporting Act, 15 U.S.C. § 168, *et seq.* ("FCRA"), to maintain the confidentiality of all consumer information. KeyPoint's Privacy Policy states that KeyPoint safeguards confidential consumer information from unauthorized internal and external disclosure, by maintaining a secure network, limiting access to KeyPoint's computer terminals and files, and maintaining backup data in encrypted form.

B. OPM's Prior Data Breaches and Failures to Comply with Federal Cybersecurity Standards and Audit Directions

78. At least two cyberattacks against OPM were publicly disclosed in the years leading up to the Data Breaches. In 2009, OPM's website and database for USAJOBS.gov—the employment website used by the federal government—was hacked by unknown persons who gained access to millions of users' private information. In May 2012, an unknown person or group infiltrated an OPM database, stole OPM user credentials (including user IDs and passwords), and posted those credentials online.

79. In addition to these cyberattacks, OPM was and is aware that its network is the subject of at least 10 million unauthorized electronic intrusion attempts every month.

80. At all relevant times, OPM also was aware of several successful cyberattacks against other federal agencies and government institutions. OPM was aware of at least the following data breach incidents: a May 2012 hack into the Bureau of Justice Statistics of the

Department of Justice, a May 2012 hack of the Thrift Savings Plan, a June 2012 hack of the Commodity Futures Trading Commission network, a June 2012 incursion into a Department of Homeland Security website, and a September 2012 breach of personnel data maintained by the Navy.

i. The Inspector General's Annual FISMA Audits of OPM

81. From 2002 to 2014, the Federal Information Security Management Act governed software system requirements for federal agencies and contractors. 44 U.S.C. § 3541, *et seq.* The President signed the Federal Information Security Modernization Act of 2014 into law on December 18, 2014. That statute updates and supersedes the Federal Information Security Management Act. As used in this Complaint, "FISMA" means either the Federal Information Security Management Act of 2002 or the Federal Information Security Modernization Act of 2014, or both.

82. FISMA requires OPM to develop and implement policies, procedures, and guidelines on information security, and to comply with federal information security standards that FISMA makes compulsory and binding on OPM.

83. Agencies subject to FISMA must develop, implement, and maintain a security program that assesses information security risks and provides adequate security for the operations and assets of programs and software systems under agency and contractor control.

84. The IG, an independent office within OPM, conducts annual audits of OPM's cybersecurity program and practices in accordance with FISMA reporting requirements established by the Department of Homeland Security.

85. The purpose of the IG's audit function is to evaluate and ensure OPM's compliance with the information security requirements of FISMA. Pursuant to FISMA, the IG is required to review several facets of OPM's information security program.

86. In each annual audit from 2011 to 2014, the IG found that OPM maintained an adequate capital planning and investment program for funding information security. In each of those years, however, the IG found that OPM had not fulfilled its information security obligations under federal law.

87. In the reporting of audit results, non-negligible security concerns of the IG are termed "significant deficiencies." More serious concerns that the IG determines pose an immediate risk to the security of assets or operations are termed "material weaknesses."

88. In each annual audit from 2007 to the present, the IG found that OPM's information security policies and practices suffered from material weaknesses.

89. Due to these material weaknesses and other information security deficiencies, OPM failed to comply with FISMA from 2007 to the present.

ii. Material Weaknesses Relating to Information Security Governance

90. OPM officials knew for several years before the OPM Breaches that OPM's information security governance and management protocols were not in compliance with FISMA. OPM officials knew for several years before the OPM Breaches that OPM's information security governance and management protocols contained material weaknesses that posed a significant threat to its systems. OPM failed to materially correct the deficiencies reported by the IG in these areas.

91. From 2007 to 2009, the IG found that OPM lacked required policies and procedures for managing information security. In 2009, the IG also found that, to the extent information security policies and procedures did exist at OPM, they had not been tailored to OPM with appropriate procedures and implementing guidance.

92. In 2009, the IG expanded the material weakness rating to cover OPM's overall information security governance program and information security management structure. A Flash Audit Alert from the IG in May 2009 identified four primary deficiencies:

a. OPM misrepresented the status of its information security program;

b. OPM's security policies and procedures were severely outdated;

c. OPM's security program was understaffed; and

d. OPM had been operating for over 14 months without a senior information security official.

93. In the 2010 FISMA audit, the IG again found that OPM's information security governance constituted a material weakness. In the 2010 FISMA audit, the IG faulted OPM for failing to remedy or otherwise address most of the deficiencies found in the 2007, 2008, and 2009 audits. OPM's policies, according to the IG, failed to provide employees with adequate guidance to secure OPM's information systems. In response, OPM stated its intent to implement comprehensive information security and privacy changes in fiscal year 2011.

94. In the 2011 FISMA audit, the IG found that OPM still lacked necessary security policies and procedures, including for agency-wide risk management, monitoring of security controls, and oversight of systems operated by a contractor. OPM's security policies again were not tailored to OPM's systems and were unaccompanied by needed guidance. The IG determined that OPM lacked a centralized security structure. Officials at various OPM divisions were responsible for testing and maintaining their own information security measures, without the guidance or oversight of the Chief Information Officer. The IG advised OPM to centralize its management structure to ensure coordinated implementation of needed information security upgrades. The IG also found that many of OPM's information security officers were not actually

information security professionals. These officers had been tasked with security functions in addition to their other full-time roles at OPM. The IG reported that OPM still was not providing appropriate guidance to its employees concerning management of systems risks.

95. By 2012, OPM had begun hiring information security professionals and centralizing its information security management structure. Nevertheless, the IG maintained its material weakness rating in its 2012 audit. In that audit the IG stated that OPM had only hired enough information security professionals to manage about one-third of OPM's information systems and that the new professionals had not performed any tangible work.

96. OPM contested the 2012 material weakness rating on the grounds that it had not suffered any loss of financial or personal information. The IG rejected OPM's position, stating that OPM's systems had, in fact, been breached on numerous occasions, resulting in the loss of sensitive data.

97. In 2013, the IG reiterated its material weakness rating of OPM's information security governance. The IG also noted that, since its last audit, OPM had not hired more security officers, thereby failing to remedy or otherwise address a central IG concern from previous years.

98. The IG's 2014 audit found that OPM still lacked a centralized cybersecurity team of individuals responsible for overseeing all of OPM's cybersecurity efforts and that OPM remained non-compliant with many FISMA requirements. The IG upgraded OPM's information security governance program from a "material weakness" to a "significant deficiency" rating, based on imminently planned improvements. The IG warned that it would reinstate the material weakness rating as to information security governance if the proposed changes were not made.

iii. Material Weaknesses Relating to Security Assessments and Authorizations of OPM Systems

99. FISMA requires OPM to certify that its information systems' technological security controls meet applicable requirements and to decide whether to authorize operation of an information system and accept the associated risk. FISMA's requirement that OPM certify and accredit system security controls is known as Security Assessment and Authorization.

100. The IG's 2010 FISMA audit found that OPM's process for certifying and accrediting system security controls was incomplete, inconsistent, of poor quality, and characterized by material weaknesses. The deficiencies stemmed in part from the fact that OPM's security officers lacked information security experience and training and were not subject to a centralized security management structure. Six OPM systems had expired authorizations in 2010, and another system had been in use for several years without being validly authorized.

101. In 2014, the IG reinstated the material weakness rating after having removed OPM's process for certifying and accrediting system security controls as a security concern in 2012 and 2013. Of the 21 OPM systems due to be authorized in 2014, eleven authorizations had not been completed. The IG recommended that OPM levy administrative sanctions on several OPM divisions, including Federal Investigative Services, whose systems were operating without valid authorizations.

102. The OPM systems operating without authorizations in 2014 included some of OPM's most critical and sensitive applications. One was a general system that supported and provided the electronic platform for approximately two-thirds of all information systems operated by OPM. Two other OPM systems operating without authorizations in 2014 were used by OPM's Federal Investigative Services division. Weaknesses in the information systems of this division, the IG warned OPM, raised national security implications.

103. The IG determined in 2014 that the lack of valid authorizations of OPM's systems was a critical and time-sensitive problem. The IG found OPM had failed to ensure that the security controls for its systems were working. The IG also found OPM lacked a way to monitor these systems for cyberattacks or data breaches. Based on these findings, the IG advised OPM to shut down all systems lacking a current and valid authorization. The IG's advice was unprecedented.

104. OPM chose not to follow the IG's 2014 recommendation to shut down the unauthorized systems.

iv. Other Deficiencies in OPM's Security Controls

105. OPM officials were aware of several other information security deficiencies summarized below. The deficiencies summarized below existed within OPM's systems immediately prior to the OPM Breaches. Each was identified and described in IG audits.

106. OPM failed to implement or enforce multi-factor authentication. OPM's failure to implement or enforce multi-factor identification increased the risk of a breach of OPM's information systems. Multi-factor authentication improves data security because a user needs more than one form of credential to access software systems. For example, the user inputs a password and also scans a PIV card with an embedded microchip. In 2011, Homeland Security Presidential Directive 12 and OMB Memorandum M-11-11 became binding on OPM. Homeland Security Presidential Directive 12 and OMB Memorandum M-11-11 require OPM to implement multi-factor authentication with PIV for its information systems. Immediately prior to the OPM Breaches, none of OPM's major information systems required PIV authentication.

107. OPM failed to promptly patch or install security updates for its systems. OPM's failure to patch or install security updates increased the vulnerability of OPM's systems to breach.

108. OPM lacked a mature vulnerability scanning program to find and track the status of security weaknesses in its systems. OPM lacked a centralized network security operations center to continuously monitor security events, and failed to continuously monitor the security controls of its software systems.

109. When employees accessed OPM's systems from a remote location, the remote access sessions did not terminate or lock out as required by FISMA. As a result, connections to OPM's systems were left open and vulnerable.

110. OPM lacked the ability to detect unauthorized devices connected to its network.

111. OPM failed to engage in appropriate oversight of its contractor-operated systems.

112. OPM failed to comply with several standards to which FISMA requires it to adhere, including in the areas of risk management, configuration management, incident response and reporting, continuous monitoring management, and contingency planning. 40 U.S.C. § 11331.

113. Only 37 of OPM's 47 software systems had been adequately tested for security in 2014, and it had been over eight years since all systems were tested.

C. Cyber Attackers Breach the Systems of OPM's Contractors

114. In or around December 2013, cyber attackers breached the information systems of KeyPoint and U.S. Investigations Services ("USIS") without being detected. At the time, KeyPoint and USIS were the primary contractors responsible for conducting the fieldwork for OPM's background and security clearance investigations.

115. In June 2014, USIS detected a breach of its systems and informed OPM that thousands of government employees' personal information might have been compromised. USIS ultimately sent out 31,000 notices of this data breach to federal employees.

116. Following the USIS breach, OPM rescinded its contracts with USIS. At the time, USIS was performing approximately 21,000 background checks per month. KeyPoint doubled the size of its work force to staff its additional responsibilities. KeyPoint failed to concurrently increase managerial oversight given its increased staff and additional responsibilities.

117. The December 2013 KeyPoint Breach was detected in September 2014. The nature and scope of the KeyPoint Breach indicate that the intrusion was sophisticated, malicious, and carried out to obtain sensitive data for improper use.

118. Following the disclosure of the KeyPoint Breach, the United States Customs Service and Border Protection suspended all investigations being conducted on its behalf by KeyPoint until KeyPoint took steps to protect GII in and connected to KeyPoint's systems.

119. OPM did not suspend KeyPoint's investigations, rescind its contract with KeyPoint, prevent or limit KeyPoint's access to OPM systems, or take any measure adequate to mitigate the potential adverse effects of the KeyPoint Breach.

120. On April 27, 2015, OPM alerted more than 48,000 federal employees that their personal information might have been exposed in the KeyPoint Breach.

121. KeyPoint lacked software logs to track malware entering its systems and data exiting its systems. Precisely how the KeyPoint Breach occurred has not been disclosed.

122. By unreasonably failing to safeguard its security credentials and Plaintiffs' and Class members' GII, KeyPoint departed from its mandate, exceeded its authority, and breached its contract with OPM.

123. The contract between OPM and KeyPoint incorporates the requirements of the Privacy Act. 5 U.S.C. § 552a(m)(1). KeyPoint violated the Privacy Act and breached its contract with OPM by failing to ensure the security and confidentiality of records and to protect

against known and anticipated threats or hazards to their security or integrity which could cause substantial harm, embarrassment, inconvenience, or unfairness to Plaintiffs and Class members. KeyPoint also violated the Privacy Act and breached its contract with OPM by disclosing Plaintiffs' and Class members' records without their prior written consent for no statutorily permitted purpose.

124. In addition to departing from the commands and directives of federal law, KeyPoint acted negligently in performing its obligations under its contract with OPM.

D. Cyber Attackers Breach OPM's Systems

i. The Information Technology Documents Breach (November 2013)

125. On November 1, 2013, OPM's network was infiltrated. No GII was stolen. The hackers stole security system documents and electronic manuals concerning OPM's information technology assets. The stolen information provided a blueprint to OPM's network.

126. When OPM later announced this breach to the public, OPM disclosed only that no GII had been compromised; it did not disclose the theft of its security system documents and information technology manuals.

ii. The Background Investigation Breach (May 2014)

127. On May 7, 2014, hackers accessed OPM's network using stolen KeyPoint credentials. Once inside OPM's network, they installed malware and created a conduit through which data could be exfiltrated.

128. The nature and scope of the May 2014 breach indicate that the intrusion was sophisticated, malicious, and carried out to obtain sensitive information for improper use.

129. The May 2014 breach was not detected for almost a year. It resulted in the theft of nearly 21.5 million background investigation records, including many million questionnaire

forms containing highly sensitive personal, family, financial, medical, and associational information of Class members.

130. The two primary systems the hackers targeted, and from which they removed data, were (i) the Electronic Official Personnel Folder system, and (ii) the database associated with the EPIC software used by the Federal Investigative Services office to collect information for government employee and contractor background checks.

iii. The Personnel Records Breach (October 2014)

131. No later than October 2014, hackers launched another successful cyberattack against OPM systems maintained in an Interior Department shared-services data center. The October 2014 breach resulted in the loss of approximately 4.2 million federal employees' personnel files.

132. The nature and scope of the October 2014 breach indicate that the intrusion was sophisticated, malicious, and carried out to obtain sensitive data for improper use.

133. Because OPM's systems were not shielded through multi-factor authentication or privileged access controls, the hackers were able to use the stolen KeyPoint credentials to access systems within OPM's network at will. During the several months in which the intruders maintained such access, they removed millions of personnel records via the Internet, hidden among normal traffic.

E. Causes of the OPM Breaches

134. Millions of unauthorized attempts to access sensitive United States government data systems take place each month. OPM's prioritization of accessibility and convenience over security foreseeably heightened the risk of a successful intrusion into OPM's systems. OPM's decisions not to comply with FISMA requirements for critical security safeguards enabled hackers to access and loot OPM's systems for nearly a year without being detected.

135. OPM's inadequate patching of software systems contributed to the OPM Breaches. When a security flaw in a software system is discovered, the developer of that system often will create and recommend installing an update—or "patch"—to eliminate that vulnerability. Failure to promptly install such a patch exposes a software system to known and preventable risks. In multiple FISMA audits, the IG found that OPM was not adequately patching its software systems and that its failure to do so represented an information security deficiency.

136. Other known deficiencies that contributed to the OPM Breaches include OPM's failures to establish a centralized management structure for information security, to encrypt data at rest and in transit, and to investigate outbound network traffic that did not conform to the Domain Name System ("DNS") Protocol.

137. Additionally, OPM's sub-networks were not segmented through the use of privileged access controls or multi-factor authentication. OPM's failure to implement such tiered identity management controls for system administrators exposed hundreds of its sub-networks, instead of a single sub-network, to breach. Had OPM implemented such controls, as required by OMB Memorandum M-11-11, the intrusion would have been detected earlier and the cyber thieves prevented from accessing the entire OPM network.

F. Announcements of the OPM Breaches

138. On June 4, 2015, OPM announced the October 2014 breach. OPM disclosed that the breach had resulted in the exposure and theft of the GII of approximately 4.2 million current, former, and prospective federal employees and contractors.

139. On June 12, 2015, OPM announced that the scope of the incident was broader than it had initially disclosed and that the GII of as many as 14 million current, former, and prospective federal employees and contractors had likely been exposed and stolen.

140. On July 9, 2015, OPM announced that the GII of approximately 21.5 million people had been exposed and stolen in the May 2014 breach. OPM disclosed that, of these compromised records, 19.7 million concerned individuals who had undergone federal background checks. OPM also disclosed that some of these records contained findings from interviews conducted by background investigators, as well as approximately 1.1 million fingerprints. OPM stated that the remaining 1.8 million compromised records concerned other individuals: mostly job applicants' spouses, children, and other cohabitants.

141. On September 23, 2015, OPM announced that it had underestimated the number of compromised fingerprints, and that approximately 5.6 million fingerprints had been exposed and stolen in the cyberattacks on its systems.

142. Prior to OPM's announcements of the Data Breaches, Plaintiffs and Class members lacked notice that their GII might have been the subject of an unauthorized disclosure. Prior to these announcements, Plaintiffs and Class members did not have a reasonable basis to suspect or believe that such an unauthorized disclosure had occurred. Plaintiffs and Class members only learned that their GII had in fact been compromised when they subsequently received written notification from OPM.

G. What the Compromised Records Contain

143. The records taken in the Data Breaches are of the utmost sensitivity. Their theft violates the privacy rights and compromises the safety of tens of thousands of individuals, including covert intelligence agents.

144. Highly sensitive personal information was exposed and stolen in the Data Breaches. Among the compromised information:

- Residency details and contact information;
- Marital status and marital history;
- Private information about children, other immediate family members, and relatives;
- Information about financial accounts, debts, bankruptcy filings, and credit ratings and reports;
- Identities of past sexual partners;
- Findings from interviews conducted by background check investigators;
- Character and conduct of individuals as reported by references;
- Social Security numbers and birthdates of applicants and their spouses, children, and other cohabitants;
- Educational and employment history;
- Selective service and military records;
- Identities of personal and business acquaintances;
- Foreign contacts, including with officials and agents of foreign governments;
- Foreign travel and activities;
- Passport information;
- Psychological and emotional health information;
- Responses to inquiries concerning gambling compulsions, marital troubles, and past illicit drug and alcohol use;
- Police and arrest records;

- Association records;
- Investigations and clearance records;
- Information relating to criminal and non-criminal legal proceedings; and
- Financial and investment records.

145. The Electronic Official Personnel Folders stolen in the OPM Breaches include employee performance records, employment history, employment benefits information, federal job applications, resumes, school transcripts, documentation of military service, and birth certificates.

146. Stolen federal job applications and investigation forms contain, among other information, Social Security numbers, birthdates, birthplaces, other names used, mailing addresses, and financial records that include bank account and credit card information.

147. Also stolen was so-called adjudication information that federal investigators gather on those who apply for positions requiring heightened security clearance, such as positions in intelligence services. Adjudication information includes the results of polygraph examinations and the details of previous confidential work, as well as intimate personal facts. Exposure of this information imperils the safety of those who work covertly to protect American interests around the world.

H. OPM Remedial Measures

148. Following the Data Breaches, OPM notified people whose GII was compromised and offered them free identity theft protection services for a limited period of time. Specifically, OPM emailed federal employees whose GII was compromised, offering identity theft protection services via a link in the email. After some federal employees received unauthorized duplicates

of these notification emails with false links that asked them to divulge personal information, OPM stopped sending notifications by email, and began sending paper notifications in the mail.

i. The Services Being Offered

149. OPM hired CSID and ID Experts—companies specializing in fraud resolution and identity theft protection—to provide services to individuals affected by the OPM Breaches.

150. At a combined cost of approximately $154 million, these companies agreed to provide victims with fraud monitoring and identity theft protection, insurance, and restoration services for either 18 months or three years, depending on the amount and sensitivity of the compromised GII.

151. OPM refers data breach victims who wish to receive additional protection to identitytheft.gov, a website managed by the FTC. That website recommends that individuals with compromised Social Security numbers purchase a credit freeze to ensure that no one can pull or modify a credit report. A credit freeze typically costs between $5 and $15. This remedial option is not included in the package being offered by OPM.

ii. OPM's Post-Breach Cybersecurity Measures Leave OPM's Systems Exposed to Further Attack

152. The IG's November 2015 FISMA audit concluded that a lack of compliance "seems to permeate" OPM's information security regime and that "OPM continues to fail to meet FISMA requirements." The IG found that OPM had followed less than half of the recommendations in the 2013 and 2014 audits, and that 21 of the 27 recommendations in the 2015 audit had been outstanding for at least a year. The IG noted that its recommendations garnered little attention even when they were repeated year after year and accompanied by warnings that OPM's failures to act magnified the risk of a data breach.

153. The IG found in November 2015 that OPM's management of its systems authorization program had regressed and would continue to be classified as a material weakness. The IG determined that up to 23 major OPM information systems were operating without a valid authorization, whereas there were eleven such systems in 2014. The IG stated that it was "very concerned" about another attack occurring and that OPM's conscious decision not to ensure valid authorizations for its systems was "irresponsible," and an "extremely poor decision."

154. In its 2015 audit, the IG again recommended that OPM shut down information systems operating without valid authorizations. OPM again refused, and it continues to operate information systems that lack valid authorizations.

155. The IG further found in November 2015 that OPM continued to lack a mature continuous monitoring program and that the security controls for its newly installed monitoring program had not been appropriately tested. On a scale of 1 to 5, with 1 being the least effective, the IG found that OPM's continuous monitoring program was functioning at level 1—"Ad-Hoc."

156. With regard to multi-factor authentication, the IG found in November 2015 that while OPM required multi-factor authentication for laptops and other devices connecting to OPM's systems, none of OPM's major applications required multi-factor authentication as required by OMB Memorandum M-11-11.

157. The IG's November 2015 audit also reported a continuing failure by OPM to provide adequate security training to many individuals responsible for the security of the information under OPM's control.

iii. Post-Breach Changes in OPM's Leadership Leave OPM without a Chief Information Officer and a Director Authorized to Act

158. On July 10, 2015, Katherine Archuleta, Director of OPM, resigned.

159. Also on July 10, 2015, the President appointed Beth F. Cobert—then the Deputy Director for Management of the Office of Management and Budget—to serve as Acting Director of OPM. On November 10, 2015, the President appointed Cobert to serve as Director of OPM.

160. On February 10, 2016, the IG informed Cobert that the Federal Vacancies Reform Act prohibits her from serving as Acting Director of OPM, because she was never a "first assistant" to the Director of OPM. 5 U.S.C. § 3345(b).

161. The IG further informed Cobert that, under 5 U.S.C. § 3348(d), any actions taken by her since her nomination are void and may not be subsequently ratified. The IG stated that "these actions may be open to challenges before the federal district court for the District of Columbia."

162. On February 22, 2016, two days before she was scheduled to testify before the House Committee on Oversight and Government Reform, Donna Seymour, Chief Information Officer of OPM, resigned. As of this filing, a replacement has not been appointed.

V. PLAINTIFFS' AND CLASS MEMBERS' DAMAGES

163. As a result of Defendants' violations of law, Plaintiffs and Class members have sustained and will continue to sustain economic loss and other harm. They have experienced and/or face an increased risk of experiencing the following forms of injuries:

A. money and time expended to prevent, detect, contest, and repair identity theft, fraud, and other unauthorized uses of GII, including by identifying, disputing, and seeking reimbursement for fraudulent activity and canceling compromised financial accounts and associated payment cards;

B. money and time lost as a result of fraudulent access to and use of their financial accounts, some of which accounts were never reimbursed;

C. loss of use of and access to their financial accounts and/or credit;

D. diminished prospects for future employment and/or promotion to positions with higher security clearances as a result of their GII having been compromised;

E. money and time expended to order credit reports and place temporary freezes on credit, and to investigate options for credit monitoring and identity theft protection services;

F. money and time expended to avail themselves of assets and/or credit frozen or flagged due to misuse;

G. impairment of their credit scores, ability to borrow, and/or ability to obtain credit;

H. money and time expended to ameliorate the consequences of the filing of fraudulent income tax returns, including by completing paperwork associated with the reporting of fraudulent returns and the manual filing of replacement returns;

I. lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breaches, including efforts to research how to prevent, detect, contest, and recover from misuse of GII;

J. anticipated future costs from the purchase of credit monitoring and identity theft protection services once the temporary services being offered by OPM expire;

K. loss of the opportunity to control how their GII is used;

L. continuing risks from the unmasking of confidential identities; and

M. continuing risks to their GII and that of their family members, friends, and associates, which remains subject to further harmful exposure and theft as long as OPM fails to undertake appropriate, legally required steps to protect the GII in its possession.

VI. CLASS ACTION ALLEGATIONS

164. Plaintiffs bring this lawsuit as a class action on their own behalf and on behalf of all other persons similarly situated as members of the proposed Class, pursuant to Federal Rules of Civil Procedure 23(a) and (b)(3), and/or (b)(1), (b)(2), and/or (c)(4). This action satisfies the numerosity, commonality, typicality, predominance, and superiority requirements.

165. The proposed Class is defined as:

> All current, former, and prospective employees of the federal government and its contractors, and their family members and cohabitants, whose sensitive personal information was compromised as a result of the breaches of OPM's electronic information systems in 2014 and 2015 or the breach of KeyPoint's electronic information systems in 2013 and 2014.

The proposed Questionnaire Subclass is defined as:

> All Class members who submitted SF-85, SF-85P, or SF-86 forms.

The proposed KeyPoint Subclass is defined as:

> All Class members who were the subject of KeyPoint investigations.

Excluded from the proposed Class and Subclasses are:

a. Senior officers, officials, and executives of Defendants and their immediate family members; and

b. Any judicial officers to whom this case is assigned and their respective staffs.

Plaintiffs reserve the right to amend the Class definition if discovery and further investigation reveal that the Class should be expanded, divided into further subclasses, or modified in any other way.

Numerosity and Ascertainability

166. The size of the Class can be estimated with reasonable precision, and the number is great enough that joinder is impracticable.

167. The number of Class members is in the millions. The disposition of their claims in a single action will provide substantial benefits to all parties and to the Court.

168. Class members are readily ascertainable from information and records in the possession, custody, or control of Defendants. Notice of this action can be readily provided to the Class.

Typicality

169. Plaintiffs' claims are typical of the claims of the Class in that the sensitive personal information of the representative Plaintiffs, like that of all Class members, was compromised in the Data Breaches.

Adequacy of Representation

170. Plaintiffs are members of the proposed Class and will fairly and adequately represent and protect its interests. Plaintiffs' counsel are competent and experienced in class action and privacy litigation and will pursue this action vigorously. Plaintiffs have no interests contrary to or in conflict with the interests of Class members.

Predominance of Common Issues

171. Common questions of law and fact exist as to all members of the Class and predominate over any questions solely affecting individual Class members. Among the questions of law and fact common to the Class are:

(a) Whether OPM, in violation of the Privacy Act, failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against anticipated threats to their security and integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to Plaintiffs and Class members;

(b) Whether OPM, in violation of the Privacy Act, disclosed Plaintiffs' and Class members' GII without their prior written consent for no statutorily permitted purpose;

(c) Whether OPM's decisions not to follow the IG's directions concerning FISMA requirements for information security constitute intentional or willful violations;

(d) Whether OPM entered into, and breached, contracts with Plaintiffs and Questionnaire Subclass members to properly safeguard their GII;

(e) Whether OPM's conduct violated the Administrative Procedure Act and, if so, what equitable remedies should issue;

(f) Whether KeyPoint owed, and breached, duties to Plaintiffs and Class members to implement reasonable and adequate cybersecurity measures and to promptly alert them if their GII was compromised;

(g) Whether KeyPoint acted negligently in failing to disclose, and falsely representing, material facts relating to its cybersecurity precautions;

(h) Whether KeyPoint's cybersecurity failures and their proximate results are highly offensive to a reasonable person in Plaintiffs' and Class members' position;

(i) Whether KeyPoint violated FCRA and, if so, what statutory remedies should issue;

(j) Whether KeyPoint engaged in unfair or deceptive acts or practices in the course of its business;

(k) Whether KeyPoint entered into, and breached, contracts with Plaintiffs and KeyPoint Subclass members to properly safeguard their GII; and

(l) Whether Plaintiffs and Class members are entitled to damages and declaratory and injunctive relief.

Superiority

172. A class action is superior to all other available methods for the fair and efficient adjudication of this controversy. Absent a class action, most Class members would likely find the cost of litigating their claims prohibitively high and would have no effective remedy. Because of the relatively small size of the individual Class members' claims, it is likely that few, if any, Class members could afford to seek redress for Defendants' violations.

173. Class treatment of common questions of law and fact would also be a superior method to piecemeal litigation in that class treatment will conserve the resources of the courts and will promote consistency and efficiency of adjudication.

174. Classwide declaratory, equitable, and injunctive relief is appropriate under Rule 23(b)(1), (b)(2), and/or (c)(4) because Defendants have acted on grounds that apply generally to the Class, and inconsistent adjudications would establish incompatible standards and substantially impair the ability of Class members and Defendants to protect their respective interests. Classwide relief assures fair, consistent, and equitable treatment of Class members and Defendants.

VII. CLAIMS FOR RELIEF

FIRST CLAIM FOR RELIEF
(Against OPM)
Violations of the Privacy Act of 1974, 5 U.S.C. § 552a

175. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

176. OPM is an agency within the meaning of the Privacy Act.

177. OPM obtained and preserved Plaintiffs' and Class members' GII, including GII contained in SF-85, SF-85P, and SF-86 forms, in a system of records.

178. In violation of the Privacy Act, OPM willfully and intentionally failed to comply with FISMA. OPM's violations of federal law adversely affected Plaintiffs and Class members. Despite known and persistent threats from cyberattacks, OPM allowed multiple "material weaknesses" in its information security systems to continue unabated. As a result, Plaintiffs' and Class members' GII under OPM's control was exposed, stolen, and misused.

179. IG reports repeatedly warned OPM officials that OPM's systems were highly vulnerable to cyberattacks and not in compliance, in several specific ways, with the Privacy Act, FISMA, and other rules and regulations governing cybersecurity at OPM. OPM officials knew that these warnings were well-founded: among other things, OPM suffered successful

cyberattacks in 2009 and 2012. OPM officials were also aware that each month saw more than 10 million attempted electronic incursions against its information systems. OPM officials, however, decided not to take adequate, legally required measures to protect the data with which the agency had been entrusted.

180. OPM was required—but failed—to take many steps to comply with controlling information security rules and regulations. OPM declined to implement PIV multi-factor authentication for all 47 of its major applications, as required by OMB Memorandum M-11-11 and as stated in the IG's audit reports. OPM affirmatively refused to shut down faulty systems even after the IG notified OPM that it was required to do so under FISMA. OPM's violations of applicable federal law include its willful failures to ensure that all operating software systems receive valid authorizations; to centralize its cybersecurity structure to provide effective management of its information systems; to monitor those systems continuously and create internal firewalls to limit the adverse effects of a breach; and to adequately train its employees responsible for cybersecurity. OPM intentionally disregarded IG findings that each of these failures rendered the agency not in compliance with federal requirements.

181. In violation of the Privacy Act and FISMA, OPM intentionally failed to comply with many other standards promulgated under 40 U.S.C. § 11331, including with regard to risk and configuration management, incident response and reporting, contractor systems, security capital planning, and contingency planning. OPM's actions were calculated to downplay the scope of the OPM Breaches and to preserve data accessibility to the detriment of data confidentiality and integrity. OPM did not destroy GII where permitted, and allowed GII to be accessible to unauthorized third parties.

182. In a continuous course of wrongful conduct, OPM willfully refused to implement electronic security safeguards required by law. OPM willfully failed to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could cause substantial harm, embarrassment, inconvenience, or unfairness to Plaintiffs and Class members, in violation of 5 U.S.C. § 552a(e)(10).

183. As a direct and proximate result of its non-compliance with federal requirements and its intentional disregard of the IG's findings under FISMA, OPM willfully disclosed Plaintiffs' and Class members' records without their prior written consent for no statutorily permitted purpose, in violation of 5 U.S.C. § 552a(b).

184. OPM's willful and intentional violations of federal law continue. OPM has failed to undertake compulsory security precautions to safeguard Plaintiffs' and Class members' GII.

185. Plaintiffs and Class members have sustained and will continue to sustain actual damages and pecuniary losses directly traceable to OPM's violations set forth above. Plaintiffs and Class members are entitled to damages under 5 U.S.C. §§ 552a(g)(1)(D) and (g)(4).

SECOND CLAIM FOR RELIEF
(Against the United States)
Breach of Contract within the Little Tucker Act, 28 U.S.C. § 1346(a)

186. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

187. Plaintiffs bring this cause of action on behalf of the Questionnaire Subclass.

188. Plaintiffs and Questionnaire Subclass members entered into valid and binding contracts with OPM.

189. OPM offered to ensure the confidentiality of Plaintiffs' and Questionnaire Subclass members' sensitive personal information in exchange for their submission of information needed by the government to conduct investigations. The SF-85, SF-85P, and SF-86 forms state that the government derives the benefit from this exchange of, among other things, being able to conduct background investigations, reinvestigations, and/or continuous evaluations of persons under consideration for, or under consideration for retention of, federal government or contractor positions, or of persons requiring eligibility for access to classified information.

190. Plaintiffs and Questionnaire Subclass members agreed to provide their sensitive personal information in return for the opportunity to be considered for government employment opportunities. Plaintiffs and Questionnaire Subclass members agreed to provide their sensitive personal information on the condition and with the reasonable understanding that—as stated in the SF-85, SF-85P, and SF-86 forms—"the information will be protected from unauthorized disclosure." OPM promised not to disclose such information without their consent, except for eleven enumerated "routine uses" and as permitted by the Privacy Act. Plaintiffs and Questionnaire Subclass members accepted the government's offer, by providing their sensitive personal information to the government in SF-85, SF-85P, or SF-86 forms.

191. At all relevant times, the agents and representatives of OPM had actual authority to act on behalf of OPM and to bind the United States. Federal statutes, agency regulations, and executive orders conferred authority on OPM to obtain this information.

192. A contract existed between OPM and Plaintiffs and Questionnaire Subclass members. When they provided their sensitive personal information to OPM, Plaintiffs and Questionnaire Subclass members reasonably expected and understood that OPM was agreeing to prevent the disclosure of such information to unauthorized third parties and/or for improper

purposes, and that OPM had the authority to enter into the agreement to prevent the disclosure of such information to unauthorized third parties and/or for improper purposes. But for this expectation and understanding, Plaintiffs and Questionnaire Subclass members would not have provided their sensitive personal information to OPM.

193. OPM did not perform on its promises to protect Plaintiffs' and Questionnaire Subclass members' sensitive personal information from unauthorized disclosure and not to disclose it for non-routine use absent their consent. Instead, in breach of its express and implied contractual obligations, OPM failed to protect Plaintiffs' and Questionnaire Subclass members' sensitive personal information from unauthorized disclosure for improper purposes.

194. OPM's breach of contract injured Plaintiffs and Questionnaire Subclass members. They are entitled to damages in an amount to be proven at trial.

195. In connection with this claim, Plaintiffs and Questionnaire Subclass members waive the right to recovery in excess of $10,000 per person.

THIRD CLAIM FOR RELIEF
(Against OPM)

Violations of the Administrative Procedure Act, 5 U.S.C. § 701, *et seq.* ("APA")

196. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

197. The APA provides for judicial review of agency actions causing legal harm or adverse effects to a plaintiff. 5 U.S.C. § 702. The APA requires the Court to deem unlawful and set aside agency actions, findings, and conclusions that are "arbitrary, capricious, an abuse of discretion, or otherwise not in accordance with law." 5 U.S.C. § 706(2)(A). The APA also requires the Court to compel agency action that has been unlawfully withheld or unreasonably delayed. 5 U.S.C. § 706(1).

198. As documented in the IG's annual audit reports, OPM acted arbitrarily and capriciously, abused its discretion, and violated the Privacy Act, FISMA, and regulations and technical standards for data security issued by the Office of Management and Budget ("OMB") and the National Institute for Standards and Technology ("NIST") that FISMA makes "compulsory and binding" on OPM.

199. Continuing to violate the APA, OPM still has not adopted or implemented a data security plan that satisfies these requirements.

200. Final agency actions of OPM prior to the OPM Breaches that were arbitrary, capricious, an abuse of discretion, and violative of applicable federal provisions and standards include OPM's decisions to:

a. operate computer and software systems without valid authorizations;

b. operate computer and software systems without requiring multi-factor authentication to access them;

c. operate computer and software systems without implementing adequate network and data segmentation;

d. operate computer and software systems without implementing layered security defenses, such as firewalls and host level anti-malware;

e. operate computer and software systems without adequately and continuously monitoring security controls and their effectiveness;

f. elect not to encrypt sensitive personal information under its control;

g. rely on a decentralized structure for governance and management of information security;

h. provide its employees with inadequate training in electronic security techniques, defenses, and protocols; and

i. operate without a comprehensive inventory of its servers, databases, and network devices.

201. The above decisions resulted from a consummation of OPM's decision making process. Judicial review is the only adequate mechanism available to correct them.

202. Final agency actions of OPM subsequent to the OPM Breaches that were arbitrary, capricious, an abuse of discretion, and violative of applicable federal requirements and standards include OPM's decisions not to:

a. shut down or otherwise isolate the compromised electronic systems;

b. undertake measures to identify, disrupt, or limit the ongoing attacks on its systems; and

c. change the access codes used to gain entry into its systems.

203. The above decisions resulted from a consummation of OPM's decision making process. Judicial review is the only adequate mechanism available to correct them.

204. OPM is under an affirmative legal obligation to promulgate and implement a data security plan that meets the standards and requirements of FISMA. In its annual audits, the IG repeatedly instructed OPM to bring its information systems into compliance with FISMA. Each year, OPM chose not to do so. For example, from 2011 to 2014, the IG advised OPM that it was not in compliance with FISMA because of its decentralized cybersecurity governance structure. OPM failed to centralize its cybersecurity governance or to otherwise bring its systems into compliance.

205. The IG audit released in November 2015 determined that OPM's cybersecurity is deficient and violative of FISMA. The IG reported, among other things, that an outbound web proxy is still missing at OPM, that controls have not been implemented to prevent unauthorized devices from connecting to the OPM network, that OPM's vulnerability management program remains substandard, and that a number of deficiencies previously identified by the IG as prone to exploitation by cyber thieves still exist within OPM.

206. OPM's current information security measures do not comply with the Privacy Act, FISMA, or the regulations and technical standards issued by the OMB and the NIST that FISMA makes "compulsory and binding" on OPM. In consequence, Plaintiffs' and Class members' GII remains at imminent risk of being exposed and stolen.

207. Plaintiffs and Class members are entitled to judicial review of OPM's actions because they have suffered legal wrongs, have been adversely affected, and remain aggrieved by OPM's final actions for which there is no other adequate remedy. Declaratory relief is warranted under 5 U.S.C. § 706(2)(A) and injunctive relief under 5 U.S.C. § 706(1).

FOURTH CLAIM FOR RELIEF
(Against OPM and KeyPoint)

Declaratory Judgment and Injunctive Relief

208. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

209. Based on Defendants' violations of law described herein, equitable relief is warranted under (i) the APA provisions referenced above, (ii) the Declaratory Judgment Act, 28 U.S.C. §§ 2201 and 2202, (iii) the common laws and statutory provisions that KeyPoint violated, and (iv) this Court's inherent authority to order equitable remedies for unlawful actions and inactions.

210. Defendants' failure to protect the GII of Plaintiffs and Class members abridged their privacy rights, resulted in concrete economic injuries, and placed millions of government workers at a heightened risk of identity theft, fraud, and other detrimental consequences.

211. Notwithstanding the IG's November 2015 identification of continuing material weaknesses and legal violations in OPM's information security protocols, OPM has not taken adequate, compulsory actions to protect Plaintiffs' and Class members' GII. OPM's continuing failure in these respects creates a substantial risk of imminent further harm to Plaintiffs, Class members, and others.

212. OPM's ongoing failure to secure its information systems and to protect the GII of current, former, and prospective federal government employees and contractors, is harmful to the public interest. The Data Breaches, and OPM's failure to properly respond to them, create a disincentive to those considering government service. By compromising the integrity of the clearance process, and by exposing the confidential information of those in sensitive government positions, OPM's unlawfully lax data security has harmed, and creates a substantial risk of further harm to, the national security of the United States. OPM's unlawfully lax data security has also led to the filing of numerous false tax returns and will continue to impose costs on the Internal Revenue Service, including by impeding its ability to collect taxes accurately and efficiently.

213. Plaintiffs seek a declaratory judgment finding unlawful the relevant conduct of Defendants and requiring them to indemnify and hold harmless any Class member who has sustained or will sustain economic injury as a result of the Data Breaches.

214. Plaintiffs further seek an injunction requiring Defendants to extend free lifetime identity theft protection services, including credit monitoring and identity theft insurance, to Plaintiffs and the Class.

215. Plaintiffs also seek an injunction requiring OPM to formulate, adopt, and implement a data security plan that satisfies the requirements of the Privacy Act and FISMA, by, among other things, mandating that all unauthorized information systems be shut down and validly authorized before being reactivated.

FIFTH CLAIM FOR RELIEF
(Against KeyPoint)

Negligence

216. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

217. It was reasonably foreseeable to KeyPoint that a breach of its information systems could occur and cause harm by compromising the GII of current, former, and prospective federal government employees. KeyPoint's and OPM's electronic systems were linked, shared, and overlapping. It was reasonably foreseeable that a breach of KeyPoint's systems would expose OPM's systems, and the GII contained therein, to a successful cyberattack.

218. KeyPoint owed a duty of care to Plaintiffs and Class members to adequately protect their GII—both in KeyPoint's network and in OPM's network—and the security credentials that could be used to access that GII. More specifically, with regard to Plaintiffs and Class members, KeyPoint was obligated to:

a. exercise due and reasonable care in obtaining, retaining, securing, protecting, and deleting GII in KeyPoint's possession;

b. exercise due and reasonable care in providing, securing, protecting, and deleting the security credentials for accessing GII on KeyPoint's and OPM's systems;

c. exercise due and reasonable care in expanding its workforce by, among other things, performing due diligence of candidates who, if hired, would have access to GII and appropriately supervising new hires;

d. safeguard GII through security procedures, protocols, and systems that are reasonable, adequate, and in conformance with recognized data security industry standards; and

e. implement procedures and protocols to promptly detect, record, mitigate, and notify the victims of data breaches.

219. KeyPoint's duties in these respects applied to Plaintiffs and Class members because they were the reasonably foreseeable victims of breaches of its information systems. KeyPoint collected and stored Plaintiffs' and Class members' GII in the course of conducting background and security clearance investigations. KeyPoint knew or should have known of the risks inherent in collecting and storing GII and the crucial importance of adequate data security, including to protect the access credentials relied on to perpetrate the Data Breaches.

220. KeyPoint owed similar duties of care to Plaintiffs and Class members under FCRA and state statutes requiring KeyPoint to reasonably safeguard Plaintiffs' and Class members' GII and to promptly notify them of any breach thereof.

221. KeyPoint's duties of care also arose from the special relationship between KeyPoint and those who entrusted it with their sensitive personal information. Plaintiffs and KeyPoint Subclass members permitted KeyPoint to access such information with the expectation that KeyPoint would take reasonable and effective precautions to protect such information from disclosure to unauthorized third parties and/or for improper purposes.

222. KeyPoint knew or should have known that its information security defenses did not reasonably or effectively protect Plaintiffs' and Class members' GII and the credentials used to access it on KeyPoint's and OPM's systems. KeyPoint's information security defenses did not conform to recognized industry standards.

223. KeyPoint's acts and omissions created a foreseeable risk of harm to Plaintiffs and Class members, breaching the duties of care it owed them. KeyPoint's breached its duties by failing to:

a. secure its systems for gathering and storing GII, despite knowing of their vulnerabilities;

b. comply with industry-standard data security practices;

c. perform requisite due diligence and supervision in expanding its workforce;

d. encrypt GII at collection, at rest, and in transit;

e. employ adequate network segmentation and layering;

f. ensure continuous system and event monitoring and recording; and

g. otherwise implement security policies and practices sufficient to protect Plaintiffs' and Class members' GII from unauthorized disclosure.

224. KeyPoint also breached its duties to Plaintiffs and Class members by failing to cause them to be promptly notified that their GII had been compromised. The KeyPoint Breach occurred in December 2013, was detected in September 2014, and was disclosed to the public on April 27, 2015.

225. But for KeyPoint's wrongful and negligent breaches of its duties of care, Plaintiffs' and Class members' GII would not have been compromised or they would have mitigated their damages more effectively.

226. Had KeyPoint promptly caused Plaintiffs and Class members to be notified of the breach of its information systems, they could have avoided or more effectively mitigated the resulting harm. They could have placed freezes and/or fraud alerts on their credit, cancelled compromised accounts, and promptly taken other security precautions to prevent or minimize the adverse consequences of GII misuse. Additionally, those whom KeyPoint began to investigate after its systems had been breached could have declined to provide their sensitive personal information to KeyPoint.

227. Plaintiffs and Class members sustained harm as a result of KeyPoint's negligence in failing to prevent and to timely cause them to be notified of the KeyPoint Breach.

228. Plaintiffs and Class members sustained harm as a result of KeyPoint's negligence in failing to protect and secure its user log-in credentials. KeyPoint's negligence in failing to protect and secure its user log-in credentials was a substantial factor in causing the Data Breaches.

229. Plaintiffs and Class members are entitled to damages in an amount to be proven at trial.

SIXTH CLAIM FOR RELIEF
(Against KeyPoint)

Negligent Misrepresentation and Concealment

230. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

231. KeyPoint owed a duty to communicate to Plaintiffs and Class members all facts within its actual or constructive knowledge that were material to KeyPoint's investigatory services as they affected Plaintiffs' and Class members' rights and interests.

232. KeyPoint breached this duty by concealing from Plaintiffs and Class members that its information security systems did not reasonably or effectively protect Plaintiffs' and Class members' GII and the credentials used to improperly access it on KeyPoint's and on OPM's systems.

233. KeyPoint knew or should have known that its information security systems did not reasonably or effectively protect Plaintiffs' and Class members' GII and the credentials used to improperly access it on KeyPoint's and OPM's systems.

234. These concealed facts were material to KeyPoint's investigatory services as they affected Plaintiffs' and Class members' rights and interests. A reasonable person in Plaintiffs' and Class members' position would expect to be notified of these facts.

235. Plaintiffs and Class members were unaware of, and had no reasonable means of discovering, these concealed facts.

236. KeyPoint falsely represented to Plaintiffs and Class members that all of its electronic systems are secure from unauthorized access and that it "maintains a secure network to safeguard consumer information from internal and external threat." KeyPoint knew or should have known that these representations were false.

237. By suppressing and misrepresenting material facts known to it alone, KeyPoint misled Plaintiffs and Class members in violation of law. KeyPoint's suppression and misrepresentation of material facts induced Plaintiffs and KeyPoint Subclass members to provide KeyPoint with their sensitive personal information or to permit KeyPoint to access their sensitive

personal information. Had KeyPoint disclosed the inadequacy of its security measures, Plaintiffs and KeyPoint Subclass members would not have provided KeyPoint with their sensitive personal information or permitted KeyPoint to access their sensitive personal information. Had KeyPoint disclosed the inadequacy of its security measures, Plaintiffs and Class members would have taken steps to prevent their injuries and/or to mitigate their damages more effectively.

238. Plaintiffs and Class members sustained economic loss as a direct and proximate result of KeyPoint's negligent misrepresentation and concealment of material facts, and are entitled to corresponding damages.

SEVENTH CLAIM FOR RELIEF
(Against KeyPoint)

Invasion of Privacy

239. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

240. Plaintiffs and Class members reasonably expected that their GII would be kept private and secure, and would not be disclosed to any unauthorized third party and/or for any improper purpose.

241. KeyPoint unlawfully invaded Plaintiffs' and Class members' privacy rights by:

a. failing to adequately secure their GII, and the user log-in credentials relied on to breach its and OPM's systems, from disclosure to unauthorized third parties for improper purposes;

b. disclosing personal and sensitive facts about them in a manner highly offensive to a reasonable person; and

c. disclosing personal and sensitive facts about them without their informed, voluntary, affirmative, and clear consent.

242. In failing to adequately secure Plaintiffs' and Class members' GII, KeyPoint acted in reckless disregard of their privacy rights. KeyPoint knew or should have known that its ineffective security measures, and their foreseeable consequences, are highly offensive to a reasonable person in Plaintiffs' and Class members' position.

243. KeyPoint violated Plaintiffs' and Class members' right to privacy under the common law as well as under the California Constitution, Article I, Section 1.

244. As a direct and proximate result of KeyPoint's unlawful invasions of privacy, Plaintiffs' and Class members' reasonable expectations of privacy were frustrated and defeated. KeyPoint's unlawful invasions of privacy damaged Plaintiffs and Class members as set forth above, and they are entitled to appropriate relief.

EIGHTH CLAIM FOR RELIEF
(Against KeyPoint)
Violations of the Fair Credit Reporting Act, 15 U.S.C. § 1681, *et seq.* ("FCRA")

245. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

246. KeyPoint recognizes in its Privacy Policy that it is a consumer reporting agency and, as such, is required by FCRA to maintain the confidentiality of all consumer information. KeyPoint is a consumer reporting agency under FCRA because, for monetary fees, it regularly engages in the practice of assembling and evaluating consumer credit information for the purpose of furnishing consumer reports to third parties (such as OPM). 15 U.S.C. § 1681a(f). KeyPoint's standard background and security clearance check procedure entails searching and analyzing the records of commercial credit reporting agencies.

247. As individuals, Plaintiffs and Class members are consumers entitled to the protections of FCRA. 15 U.S.C. § 1681a(c).

248. KeyPoint willfully violated FCRA.

249. In violation of 15 U.S.C. § 1681b(a)(3), consumer reports concerning Plaintiffs and Class members were furnished by or from KeyPoint for no statutorily permitted purpose.

250. In violation of 15 U.S.C. § 1681e(a), KeyPoint failed to maintain reasonable procedures to limit the furnishing of consumer reports to statutorily permitted purposes, in at least the following respects:

a. KeyPoint failed to undertake reasonable electronic security precautions that would have prevented the KeyPoint Breach and its unauthorized furnishing of consumer reports;

b. KeyPoint furnished consumer reports to OPM despite KeyPoint's actual or constructive knowledge of its and OPM's inadequate electronic security precautions; and

c. KeyPoint failed to undertake reasonable electronic security precautions to protect the user log-in credentials used to commit the Data Breaches, and this failure caused consumer reports to be furnished for no statutorily permitted purpose.

251. KeyPoint's violations of FCRA directly and proximately caused the exposure, theft, and misuse of Plaintiffs' and Class members' GII. Their GII stored on KeyPoint's network was compromised in the KeyPoint Breach. KeyPoint user log-in credentials were used to hack into OPM's information systems and to compromise Plaintiffs' and Class members' GII stored on OPM's network. KeyPoint's failure to secure its user log-in credentials was a substantial factor in causing the Data Breaches.

252. As a direct and proximate result of KeyPoint's violations of FCRA, Plaintiffs and Class members have sustained damages as set forth above. They are entitled to their actual

damages or statutory damages, as well as attorneys' fees and costs as may be permitted by statute.

NINTH CLAIM FOR RELIEF
(Against KeyPoint)
Violations of State Statutes Prohibiting Unfair and Deceptive Trade Practices

253. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

254. KeyPoint is engaged in trade and commerce. As relevant here, KeyPoint's acts, practices, and omissions occurred in the course of KeyPoint's business of conducting background and security clearance investigations of Plaintiffs and Class members throughout the United States.

255. KeyPoint's conduct as alleged herein constitutes unfair, deceptive, fraudulent, unconscionable, and/or unlawful acts or practices. Among other violations, KeyPoint:

a. failed to implement and maintain data security practices adequate to safeguard Plaintiffs' and Class members' GII and the security credentials used to breach its and OPM's information systems;

b. made misleading and deceptive representations and omissions in its publicly disseminated Privacy Policy regarding its ability and efforts to secure Plaintiffs' and Class members' GII;

c. failed to disclose that its data security practices and protocols were insufficient to protect Plaintiffs' and Class members' GII;

d. failed to timely disclose the KeyPoint Breach to Plaintiffs and Class members; and

e. continued to accept and store Plaintiffs' and Class members' GII even after obtaining actual or constructive notice of its security vulnerabilities.

256. By reason of its acts and omissions, KeyPoint violated the following statutes prohibiting unfair or deceptive acts or practices:

a. The California Unfair Competition Law, Cal. Bus. & Prof. Code, § 17200, *et seq.*;

b. The Florida Deceptive and Unfair Trade Practices Act, Fla. Stat. Ann. § 501.204(1), *et seq.*;

c. The Idaho Consumer Protection Act, Idaho Code Ann. § 48-603(18), *et seq.*;

d. The Illinois Consumer Fraud and Deceptive Trade Practices Act, 815 Ill. Comp. Stat. § 505/2, *et seq.*, and the Illinois Uniform Deceptive Trades Practices Act, 815 Ill. Comp. Stat. § 510/2(a)(12), *et seq.*;

e. The Nevada Deceptive Trade Practices Act, Nev. Rev. Stat. Ann. § 598.0915, *et seq.*;

f. The New Hampshire Consumer Protection Act, N.H. Rev. Stat. Ann. § 358-A:2, *et seq.*;

g. The New Mexico Unfair Practices Act, N.M. Stat. Ann. §§ 57-12-2(D)(17) & 57-12-3, *et seq.*;

h. The North Carolina Unfair Trade Practices Act, N.C. Gen. Stat. Ann. § 75-1.1(a), *et seq.*;

i. The Pennsylvania Unfair Trade Practices and Consumer Protection Law, 73 Pa. Stat. §§ 201-2(4)(xxi) & 201-3, *et seq.*;

j. The Virginia Consumer Protection Act, Va. Code Ann. § 59.1-200(A)(14), *et seq.*; and

k. The Washington Consumer Protection Act, Wash. Rev. Code Ann. § 19.86.020, *et seq.*

257. As a direct and proximate result of KeyPoint's violations of the above provisions, Plaintiffs and Class members sustained damages, as described herein, and are entitled to appropriate monetary and equitable relief as well as attorneys' fees and costs as may be permitted by statute.

258. Before filing this Complaint, counsel for Plaintiffs sent a copy of this Complaint to the Attorney General of Washington, pursuant to Wash. Rev. Code § 19.86.095.

TENTH CLAIM FOR RELIEF
(Against KeyPoint)

Violations of State Data Breach Acts

259. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

260. The KeyPoint Breach constitutes a security breach that triggered the requirements of various state data breach acts. The GII exposed and stolen in the KeyPoint Breach includes personal information protected by these statutes.

261. In violation of state data breach acts, KeyPoint unreasonably delayed in causing Plaintiffs and Class members to be notified of the KeyPoint Breach after KeyPoint knew or should have known of it. The KeyPoint Breach occurred in December 2013, was detected in September 2014, and was disclosed to the public on April 27, 2015.

262. KeyPoint's failure to cause timely notice of the KeyPoint Breach to be provided violated the following statutes:

a. Cal. Civ. Code § 1798.80, *et seq.*;

b. Ga. Code Ann. § 10-1-912(a), *et seq.*;

c. 815 Ill. Comp. Stat. 530/10(a), *et seq.*;

d. Kan. Stat. Ann. § 50-7a02(a), *et seq.*;

e. Mich. Comp. Laws Ann. § 445.72(1), *et seq.*;

f. N.H. Rev. Stat. Ann. § 359-C:20(1)(a), *et seq.*;

g. N.C. Gen. Stat. Ann. § 75-65(a), *et seq.*;

h. Tenn. Code Ann. § 47-18-2107(b), *et seq.*;

i. Va. Code Ann. § 18.2-186.6(B), *et seq.*;

j. Wash. Rev. Code Ann. § 19.255.010(1), *et seq.*; and

k. Wis. Stat. Ann. § 134.98(2), *et seq.*

263. KeyPoint's violations of these statutes damaged Plaintiffs and Class members. Had KeyPoint timely caused Plaintiffs and Class members to be notified of the breach of its information systems, they could have avoided or more effectively mitigated the resulting harm. They could have placed freezes and/or fraud alerts on their credit, cancelled compromised accounts, and promptly taken other security precautions to prevent or minimize the adverse consequences of misuse of their sensitive personal information. Additionally, those whom KeyPoint began to investigate after its systems had been breached could have declined to provide their sensitive personal information to KeyPoint.

264. In further violation of Cal. Civ. Code § 1798.80, *et seq.*, KeyPoint failed to implement and maintain security measures sufficient to prevent the KeyPoint Breach and protect the security credentials used to perpetrate the Data Breaches. KeyPoint's violations of Cal. Civ. Code § 1798.80 damaged Plaintiffs and Class members.

265. KeyPoint failed to establish appropriate procedures to ensure the confidentiality of Plaintiffs' and Class members' medical information and to protect such information from unauthorized use and disclosure, in violation of Cal. Civ. Code § 56.20-56.245, *et seq.* KeyPoint also violated Wis. Stat. §§ 146.82 and 146.84 and Va. Code § 32.1-127.1:03(3) by disclosing Plaintiffs' and Class members' medical records without specific authorization or other justification. KeyPoint's violations of Cal. Civ. Code § 56.20-56.245, *et seq.*, Wis. Stat. §§ 146.82 and 146.84, and Va. Code § 32.1-127.1:03(3) damaged Plaintiffs and Class members.

266. Based on KeyPoint's violations of the foregoing provisions, Plaintiffs and Class members are entitled to appropriate monetary and equitable relief as well as attorneys' fees and costs as may be permitted by statute.

ELEVENTH CLAIM FOR RELIEF
(Against KeyPoint)
Breach of Contract

267. Plaintiffs hereby incorporate by reference the allegations contained in the preceding paragraphs of this Complaint.

268. Plaintiffs bring this cause of action on behalf of the KeyPoint Subclass.

269. Plaintiffs and KeyPoint Subclass members entered into valid and binding contracts with KeyPoint.

270. KeyPoint offered to ensure the confidentiality of Plaintiffs and Class members' GII in exchange for their submission of information needed to conduct background and security clearance investigations. KeyPoint derived the benefit from this exchange of, among other things, being able to conduct such investigations and receiving associated payments from OPM.

271. Plaintiffs and Class members agreed to furnish their sensitive personal information to KeyPoint, or to permit KeyPoint to access it, in return for the opportunity to be

considered for government employment opportunities. Plaintiffs and Class members agreed to permit KeyPoint to access their sensitive personal information on the condition that KeyPoint would act to "secure" such information "from unauthorized access." Since October 2012 at the latest, KeyPoint continuously promised to "maintain[] a secure network to safeguard consumer information from internal and external threat." Plaintiffs and Class members accepted KeyPoint's offer, by permitting KeyPoint to access their sensitive personal information.

272. At all relevant times, the agents and representatives of KeyPoint had actual authority to act on behalf of, and to bind, KeyPoint.

273. A contract existed between KeyPoint and Plaintiffs and KeyPoint Subclass members. When they permitted KeyPoint to access their sensitive personal information, Plaintiffs and KeyPoint Subclass members reasonably expected and understood that KeyPoint was agreeing to prevent the disclosure of such information to unauthorized third parties and/or for improper purposes, and that KeyPoint's agents and representatives had the authority to enter into this agreement to prevent the disclosure of such information to unauthorized third parties and/or for improper purposes. But for this expectation and understanding, Plaintiffs and KeyPoint Subclass members would not have permitted KeyPoint to access their sensitive personal information.

274. KeyPoint did not perform on its promises to safeguard Plaintiffs' and KeyPoint Subclass members' sensitive personal information and to maintain a secure network. Instead, in breach of its express and implied contractual obligations, KeyPoint failed to undertake reasonable and appropriate security precautions. The proximate result was the KeyPoint Breach and the theft of user log-in credentials used to perpetrate the Data Breaches.

275. KeyPoint's breach of contract injured Plaintiffs and KeyPoint Subclass members. They are entitled to damages in an amount to be proven at trial.

VIII. PRAYER FOR RELIEF

WHEREFORE, Plaintiffs seek a judgment against Defendants through an Order:

A. certifying this case as a class action, designating Plaintiffs as Class and Subclass representatives, and appointing Plaintiffs' counsel to represent the Class;

B. finding Defendants liable for their failure to establish adequate and legally required safeguards to ensure the security of Plaintiffs' and Class members' GII compromised in the Data Breaches;

C. requiring Defendants to pay money damages, including actual and statutory damages, to Plaintiffs and Class members;

D. declaring that the relevant conduct of Defendants is unlawful and that Defendants shall indemnify and hold harmless any Class member who has sustained or will sustain economic injury as a result of the Data Breaches;

E. enjoining Defendants to extend free lifetime identity theft and fraud protection services, including credit monitoring and identity theft insurance, to Plaintiffs and the Class;

F. enjoining OPM to formulate, adopt, and implement a data security plan that satisfies the requirements of the Privacy Act and FISMA, by, among other things, mandating that all unauthorized information systems be shut down and validly authorized before being reactivated;

G. awarding reasonable attorneys' fees and costs as may be permitted by law;

H. awarding pre-judgment and post-judgment interest as may be prescribed by law; and

I. granting such further and other relief as may be just and proper.

IX. JURY TRIAL DEMANDED

Plaintiffs hereby demand a trial by jury on all issues so triable.

DATED: March 14, 2016

Respectfully submitted,

GIRARD GIBBS LLP

By: /s/ *Daniel C. Girard*
Daniel C. Girard

Jordan Elias
Esfand Y. Nafisi
Linh G. Vuong
601 California Street, 14th Floor
San Francisco, CA 94108
(415) 981-4800
dcg@girardgibbs.com

Interim Lead Class Counsel

David H. Thompson
Peter A. Patterson
Harold Reeves
COOPER & KIRK, PLLC
1523 New Hampshire Avenue, N.W.
Washington, D.C. 20036

Tina Wolfson
Theodore Maya
Bradley King
AHDOOT & WOLFSON, PC
1016 Palm Avenue
West Hollywood, CA 90069

John Yanchunis
Marcio W. Valladares
Patrick A. Barthle II
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 North Franklin Street, 7th Floor
Tampa, FL 33602

Plaintiffs' Steering Committee

Gary E. Mason
Ben Branda
WHITFIELD BRYSON & MASON LLP
1625 Massachusetts Avenue, N.W., Suite 605
Washington, D.C. 20036

Liaison Counsel

Norman E. Siegel
Barrett J. Vahle
J. Austin Moore
STUEVE SIEGEL HANSON LLP
460 Nichols Road, Suite 200
Kansas City, MO 64112

Denis F. Sheils
KOHN, SWIFT & GRAF, P.C.
One South Broad Street, Suite 2100
Philadelphia, PA 19107

Graham B. LippSmith
KASDAN LIPPSMITH WEBER TURNER LLP
500 South Grand Avenue, Suite 1310
Los Angeles, CA 90071

Nicholas Koluncich III
THE LAW OFFICES OF NICHOLAS KOLUNCICH III
500 Marquette Avenue N.W., Suite 1200
Albuquerque, NM 87102

Edward W. Ciolko
KESSLER TOPAZ MELTZER & CHECK LLP
280 King of Prussia Road
Radnor, PA 19087

Steven W. Teppler
ABBOTT LAW GROUP, P.A.
2929 Plummer Cove Road
Jacksonville, FL 32223

Plaintiffs' Counsel

EXHIBIT A

APPENDIX D of OPM FIS Security Manual

U.S. Office of Personnel Management
Federal Investigative Services

POLICY ON THE PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

August 2012

Table of Contents

1.0 Introduction and Definitions

1.1 As an employee or contractor who works for or on behalf of the United States Office of Personnel Management (OPM), Federal Investigative Services (FIS), it is your responsibility to protect all personal information that has been entrusted to you. An important part of this duty is to ensure that you properly use, protect, and dispose of Personally Identifiable Information (PII).

1.2 As an Executive Agency within the United States Government, OPM/FIS, defines PII according to the same terms defined by the Office of Management and Budget (OMB). OMB defines PII as, "information which can be used to distinguish or trace an individual's identity, such as their name, social security number, biometric records, etc. alone, or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, mother's maiden name, etc."[1]

1.3 OPM/FIS defines a reportable loss of PII as that which occurs anytime information is lost, to include temporary losses, in which the information:

- can be used to discern or trace a person's identity; and
- that alone, or combined with other information, can be used to compromise the integrity of agency records relating to a person, by permitting access to unauthorized disclosure of these records; or
- involved a laptop, portable mass storage device (i.e.: thumb drive), or any other type of information technology equipment, if PII was contained on such a device.

1.4 As defined above, in Section 1.3, the loss of information that contains strictly an individual's name, and no other accompanying information, would generally not be considered a reportable loss.

1.5 All OPM/FIS personnel and contractor personnel should limit the printing and transporting of PII whenever possible to minimize potential loss. The less hardcopy PII we have outside of our control, the more we reduce our vulnerability to a PII breach.

1.6 Chain of custody is defined as control of material pertaining to a Subject of an investigation upon receipt until PII is properly relinquished to an approved authority or properly destroyed.

1.6.1 OPM relinquishes responsibility in the chain of custody when it properly leaves our control and is transmitted to an official authorized to use the PII in order to receive information or when transferred to another Federal Agency for adjudicative or informational purposes.

- Is transmitted to an official authorized to use the PII; or
- When transferred to another Federal Agency for adjudicative or informational purposes; or
- When properly packaged and transferred to an authorized carrier.
- When it cannot be determined that PII sent to or between OPM/FIS facilities has been received at an OPM/FIS facility, it is the responsibility of the sending party to determine the disposition of the information (chain of custody status)and report any breach of PII through their respective chain of command.
- Transfer of PII responsibility/accountability occurs only if the information has been positively confirmed to have been received by the intended gaining OPM/FIS office/facility or other authorized parties.

2.0 Responsibilities

[1] OMB Memorandum 07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, dated May 22, 2007.

2.1 The Associate Director, FIS, is ultimately responsible for establishing policies and procedures that ensure the protection of all PII entrusted to OPM/FIS.

2.2 The Chief of FIS Integrity Assurance is designated as the OPM/FIS Senior PII Representative and oversees the OPM/FIS PII Program on behalf of the Associate Director. In addition to establishing and updating OPM/FIS' PII Policy, the Chief of OPM/FIS Integrity Assurance is also responsible for overseeing the handling of PII incidents and recommending notification to victim(s) whose PII has been lost or otherwise compromised.

2.3 All FIS personnel and contractors are responsible for ensuring full compliance with all PII policies. FIS personnel and contractors must immediately report any possible compromise of PII following the established reporting procedures. Failure to adhere to FIS PII Policy, to include reporting procedures, may be grounds for disciplinary or adverse action, up to and including removal.

3.0 Standards

3.1 OPM/FIS personnel, to include both Federal staff and contractors, are trusted with highly sensitive PII, the protection of which is an inherent responsibility of all personnel. OPM/FIS Standards for the protection of PII are largely based on common sense. While OPM/FIS will establish certain minimum standards of control, as defined throughout this document, OPM/FIS management recognizes the constantly changing nature and varying circumstances amongst most OPM/FIS staff, and therefore relies heavily upon its staff to exercise good judgment in the handling of PII.

3.1.1 This policy establishes minimum standards for the protection of PII. Supervisory personnel may establish stricter controls for the handling of PII based upon office location and circumstances unique to an individual area. Any additional controls placed upon individual personnel, as a result of specific circumstances, will be considered an enhancement to the mandatory minimum requirements outlined in this document.

3.1.2 FIS Personnel who have signed an individual telework agreement, which places additional measures of control, must adhere to the specific standards and policies of the individual telework agreement.

3.1.3 Any requests for variances from this policy must be submitted thru supervisory channels. Upon approval of the supervisory chain, the request will be submitted to OPM/FIS Integrity Assurance for a final determination. All variances require approval of OPM/FIS Integrity Assurance prior to implementation.

3.2 OPM/FIS Field Office and Satellite Office storage requirements:

3.2.1 Long term storage in Satellite Offices is prohibited. All case materials must be turned into the Field Offices for retention.

3.2.2 A two barrier rule applies to the protection of all PII within OPM/FIS and contractor office space.

3.2.3 The primary barrier in all OPM/FIS and contractor office space shall be a locked exterior office door, to prevent the entry of unauthorized individuals.

3.2.4 During regular office hours, staff and office personnel may serve as the second barrier for the protection of unauthorized access to PII within FIS' control.

3.2.5 When an office is not staffed (i.e., outside of core hours or when authorized staff is out of the office), PII shall be secured within a locking file cabinet or within a designated storage area behind a separately locked internal door. A locked file cabinet or separately secured internal door will serve as the second barrier during times when an office is not staffed with OPM/FIS or contractor personnel.

3.2.6 Due to the unique nature and security policies of FIS core facilities at Boyers, Ft. Meade, and the Theodore Roosevelt Building, section 3.2.5 is not applicable to these locations, due to additional security measures already in place.

3.2.7 Individuals who are not properly cleared for authorized access to OPM/FIS office space must be escorted at all times.

3.3 Domicile storage requirements:

3.3.1 Information will be secured from access by others, including family members and guests, who may access the domicile location.

3.3.2 When the domicile location is unattended and contains PII the residence must be locked.

3.3.3 All personnel will provide their first line supervisor with documentation explaining how PII is stored and protected within their residence. Documentation will be provided within 30 days of receipt of this policy and subsequently updated within 30 days of any change in domicile storage procedures. First line supervisors will maintain current copies of each employee's submission and request yearly updates from their staff. It is the responsibility of the supervisor to determine whether or not the submitted plan is acceptable.

3.4 Vehicle storage requirements:

3.4.1 Vehicles are used for the transport of PII between official locations, when such transport is required for conducting official FIS business. As such, PII will never be left in a vehicle overnight or for any other extended period of time. While it is recognized that the storage of PII in vehicles, under certain circumstances, will be unavoidable, whenever possible OPM/FIS personnel shall take PII with them and not leave it in a vehicle. While it is emphasized that only the minimum PII necessary to work productively should be carried into the field, it is recognized that some investigative activities, such as those conducted in residential areas, requires that the investigator travel lightly. Under these limited circumstances, PII may be secured in a locked trunk, as long as the information is secured in a manner that complies with sections 3.4.2 thru 3.4.6.

3.4.2 Case material will never be left unattended while in plain view or in any area other than the trunk of the vehicle.

3.4.3 The only authorized storage location for PII, within a parked vehicle, is within a locked trunk. When storing PII within a locked trunk, personnel shall take measures to place the PII in the trunk prior to arriving at their destination, so as to avoid drawing attention to the storage of materials within the trunk.

3.4.4 If the vehicle does not have a separate locking trunk area, as is such with certain sport utility vehicles, personnel will place the PII in the equivalent area of the vehicle and ensure it is covered from plain view and does not attract unusual attention.

3.4.5 Personnel will ensure the vehicle is locked and that all windows are fully closed, prior to leaving the vehicle.

3.4.6 Personnel will ensure items of value or other materials that may attract undue attention to a vehicle are secured and not within plain view (i.e., GPS units, cellular telephones, satellite radios, purses, packages, etc.).

3.5 Hotel room storage requirements:

3.5.1 Never leave material containing PII material in plain view to include laptops.

3.5.2 If available, PII should be stored in a locked safe. If no locking safe is available, PII should be stored outside of plain view.

3.5.3 If unable to adequately secure PII within a hotel room, OPM/FIS personnel should evaluate if taking the material with them for temporary storage within their vehicle is more appropriate during times when not in the hotel room.

3.6 When traveling via airline or by other commercial means, PII material, to include laptops or other information technology equipment containing PII, will never be stored within checked baggage and will remain within the control of the employee at all times.

3.7 When transporting PII between locations, it shall be contained within a closed container (i.e.: closed briefcase, zippered portfolio). PII shall not be transported in an open container, so as to reduce the potential for inadvertent loss.

4.0 PII Transmission Requirements

4.1 Upon receipt of case assignments, personnel are required to print necessary case material at their duty station, if equipped to do so. This replaces the shipment of case material by mail or other courier, whenever possible.

4.2 In the limited instance that case material is sent via the U.S. Postal Service (USPS) or other commercial carrier (e.g., UPS, FedEx, etc.), the material must be sent in such a method that allows for the item to be tracked throughout the entire shipping process. The use of a "delivery confirmation," in and of itself, will not suffice.

4.2.1 Any material sent via USPS or other commercial carrier will be fully manifested prior to sending. The manifest will contain the case names and associated numbers for all material contained within the shipment, along with any other relevant documents containing PII within the shipment. The sender of the shipment will include one copy of the manifest in the shipment and will retain a second copy, for use in the event of a lost or damaged shipment. All material will be double wrapped with the internal packaging also identifying the recipient of the information but without any markings indicating that PII is contained within the package.

4.2.2 Prior to sending any PII via USPS or other commercial carrier, the sender will notify the recipient of the shipment and its expected arrival date. Such notification shall be done via e-mail or other electronic method when possible.

4.2.3 Upon receipt of the shipment, the recipient will immediately reconcile the package contents with the enclosed manifest. Any discrepancies will be immediately reported to the sender and proper reporting requirements will be followed. Acknowledgement of the shipment shall be sent in the same manner in which the original notification of shipment was made. If the package does not arrive when expected, the recipient will notify the sender to initiate tracking of the package.

4.2.4 The shipper will retain the original manifest and recipient's confirmation for a period of two years. There is no requirement for the recipient to maintain a copy of the shipping manifest.

4.3 Transmission of PII via email:

4.3.1 Unsecure email is never to be used for transmission of PII or other case related material.

4.3.2 Messages sent within the "OPM.GOV" domain are deemed secured. Messages sent to a recipient outside of the "OPM.GOV" domain must be encrypted for secure transmission. For these purposes only, the use of a Subject's last name and the case number will not be considered PII[2].

4.4 Thumb drive or other portable media storage of PII:

[2] Reference August 20, 2009 Guidance from OPM Director John Berry, "CLARIFICATION: Procedures Regarding Personally Identifiable Information (PII) and Email Encryption"

4.4.1 Thumb drives or other portable media may be used to store PII data provided the device is issued by OPM. PII placed on the device must be encrypted.

4.5 Use of fax machines to transmit PII:

4.5.1 When faxing PII, the primary method for the transmission of PII should be a Government owned or controlled facsimile machine. When faxing material, FIS personnel should maintain visual control of the document(s) at all times. OPM/FIS Personnel and contractors will confirm the validity of fax numbers prior to sending.

4.5.2 The use of non-government or other commercial services for sending facsimiles (e.g.: FedEx Kinko's, Staples, OfficeMax, hotel business centers, etc.) is permitted when the sender is on TDY and does not have access to a government owned or controlled facsimile machine. In such instances, the sender will never relinquish control of the document and will insure accountability of the document at all times.

4.5.3 If receiving PII at a non-government or other commercial service facsimile, the recipient must be present at the time of transmission to receive the document. OPM/FIS personnel and contractors will never request a document containing PII be sent to a commercial service or other non-government location and have individuals unauthorized to view or handle FIS documents receive it for them (i.g, hotel staff, store employee, etc.).

4.5.4 OPM/FIS personnel and contractors will verify the receipt of all faxes. In cases where a machine generated delivery confirmation is available, this document shall be retained by personnel and will suffice as a delivery receipt. Personnel will store the confirmation receipt within the local case file; retention will be in accordance with current case retention policies.

4.5.5 Frequently utilized numbers should be programmed into office and other government owned/issued facsimile machines in order to reduce the likelihood of error in sending facsimiles containing PII to unauthorized personnel/locations. Programmed numbers should be periodically checked to insure they are still valid.

4.6 Websites:

4.6.1 Entering PII (Subject identifiers such as name and SSN) on public internet sites to obtain investigative results is strictly prohibited unless specific authorization is received thru appropriate procedures and the website has been authorized for such use by OPM/FIS.

4.6.2 Authorization regarding utilization of particular sites will be disseminated to personnel when the use of those sites has been approved by OPM/FIS.

4.6.3 Use of the internet is permissible for lead purposes. "Lead purposes" are those activities that may assist personnel in conducting investigations more efficiently and do not require inputting of PII for search results. Examples include locating addresses of facilities or phone numbers of individuals.

4.7 Completed cases:

4.7.1 Upon completion of cases, field personnel will expeditiously return all completed materials and case notes to the originating field office. Under no circumstances will cases be held past the 7th day of the following month (i.g., cases completed in April, must be returned no later than May 7th).

4.7.2 Supervisors may require personnel to return case materials in a more expeditious manner than referenced in Section 4.7.1; under no circumstances will personnel hold cases for a longer period than defined in Section 4.7.1.

4.7.3 Unauthorized personnel will not destroy any case materials, including case notes, and must ensure all documents are returned to the field office for appropriate reconciliation and retention. Materials will be destroyed, by the first line supervisor or his/her designee, when directed to do so thru case messaging. Personnel are not authorized to destroy case materials at their residences.

4.7.4. Supervisors will ensure materials are properly destroyed within five business days of notification to do so. Personnel will maintain destruction logs of all case materials destroyed. Destruction logs will be maintained for a period of two years.

4.7.5 Investigative personnel will delete cases from their computer(s) within five business days of being directed to do so.

5.0 Manifesting Requirements

5.1 The submission of a daily manifest to provide accountability of investigative case material in possession of personnel while moving between their duty stations and/or authorized locations is required.

5.2 Field personnel will create and submit a manifest at the start of each working day, prior to transporting any PII. In cases where no PII is being transported, OPM/FIS personnel and contractors will submit a blank manifest or otherwise document to their supervisor that no PII will be transported that day. Documentation will be submitted daily, no later than 9 a.m. local time or prior to transporting any PII.

5.2.1 Supervisory Agents-in-Charge (SAC's), or other first line supervisors, will ensure full accountability for daily manifests, as outlined above in 5.2.

5.3 Personnel with the need to transport material containing PII will be responsible for completing a detailed manifest. At a minimum, the manifest will contain the following information:

1. Date of manifest
2. Staff name
3. Case name (last), case number
4. Identification of the document(s) (case papers, release(s)/type of release(s), entire file)

5.4 Reconciliation of the manifest will be completed upon return to/arrival at the final duty location. Any discrepancies within the daily reconciliation of PII must be immediately reported as outlined in this policy.

5.4.1 Manifests will be maintained by supervisors for a period of two years from date of final receipt. Electronic storage of such manifests is acceptable.

5.5 Personnel who are in a TDY status will submit a daily manifest to both their assigned TDY supervisor and their home SAC.

6.0 Reporting a Possible PII Breach

6.1 The determination about whether PII has been breached will be done carefully but promptly to ensure that the likelihood of a breach of PII is established by the preponderance of the data available. Mere suspicion of a breach should not be reported without further follow-up to determine the exact circumstances. To assist OPM/FIS personnel and contractors in assessing the likelihood of a PII breach, the following procedures shall be followed.

6.2 In evaluating whether or not to report a breach, FIS personnel shall consider all relevant factors. Instances of theft or any other immediately known loss should be reported as such. Cases of missing packages within the USPS or other commercial carrier should be investigated further to determine the likelihood of a lost package, as opposed to one that is simply delayed. In all instances, once a loss or other breach is suspected or known, it must be immediately reported.

6.2.1 Shipments that are confirmed to have been lost or cannot be accounted for after a reasonable period of time shall be reported as lost PII.

6.2.2 Misdirected faxes and other dissemination of documents to unauthorized individuals will be reported as lost PII.

6.2.3 In cases where it is undetermined whether or not an incident should be reported, personnel shall immediately contact the Chief of OPM/FIS Integrity Assurance for further guidance and instructions.

6.2.4 The responsibility for proper follow-up and additional measures regarding the investigation and/or recovery of lost materials will be that of the first line supervisor.

6.3 Notification:

6.3.1 Within 30 minutes of a determined PII loss, the FIS supervisor of the individual responsible for the loss will contact the OPM Situation Room (SITROOM). The SITROOM is available 24 hours per day, 7 days per week. The SITROOM will be notified either telephonically at (202) 418-0111 or via email at usopmsr@opm.gov. The reporting individual will provide all known details to the SITROOM. When reporting a PII breach it must be noted if National Agency Check (NAC) items are lost for proper reporting to the originating agency.

6.3.2 When reporting information, the SITROOM requires general information to include name, location, number of cases, and general details of the incident. Specific PII of individuals should not be included (i.e. SSN).

6.3.3 Within four (4) hours from the point that the incident is reported to the SITROOM, the Supervisor of the individual believed responsible for the PII loss will coordinate with their supervisor (the second line supervisor for the employee who is believed responsible for the loss). In coordination, the individual responsible for the loss and their supervisor(s) will submit the FIS PII Loss Reporting Form to the FIS Incident Response Team, via email at FISINCIDENTRESPONSETEAM@OPM.GOV.

6.3.4 The responsible individual's Supervisor will take immediate steps to initiate recovery of the material and/or to follow up with additional parties relevant to the loss and/or recovery of PII material.

6.3.5 Supervisors are responsible for ensuring that the FIS Incident Response Team and SITROOM are immediately updated on changes to initially reported information (i.e., PII is found, lost shipment recovered, etc.).

6.3.6 If, within 60 days after the PII loss was initially reported, the status of the PII loss has not changed, or it has not been previously updated as per 6.3.4, the supervisor will provide a status update to FIS Integrity Assurance.

7.0 Official Loss Notifications

7.1 FIS Integrity Assurance will review each reported PII loss and make a determination regarding appropriate notifications. FIS' Freedom of Information and Privacy Act Office will ensure all required notifications to the affected Subject(s) are made within three days of determination, unless specific circumstances of an individual loss dictate faster notification. All notifications will conform to the required internal procedures for such.

7.2 All notifications to Subject's affected by lost PII will be made as outlined in 7.1. Personnel not associated with the official notification procedures should not notify or otherwise inform the affected Subject(s) of lost PII. Any exceptions must be coordinated thru OPM FIS Integrity Assurance and/or FIS' Freedom of Information and Privacy Act Office.

8.0 Compliance

8.1 FIS Integrity Assurance is responsible for oversight and ensuring full compliance with the established PII Policy. To ensure compliance, FIS Integrity Assurance will conduct random audits of FIS offices. All personnel must fully comply with PII Audits.

8.2 Exceptions to the standards set forth in this policy will be submitted to FIS Integrity Assurance for review and determination. No exceptions are authorized without the prior approval of FIS Integrity Assurance.

8.3 Failure to follow the FIS PII Policy may result in disciplinary action, up to and including removal.

ATTACHMENT 1

U.S. Office of Personnel Management

Federal Investigative Services

FIS PII LOSS REPORTING FORM
INITIAL NOTIFICATION

REPORTING INDIVIDUAL INFORMATION
(Information regarding individual discovering the PII incident)

Name of Reporting Individual:
Address:
Company (Contractor) or **Region** (Federal):
Telephone No.-Office: **Telephone No.-Cell**:
Email:
Date/Time [1] **the PII Incident Occurred (if known)**:
Ticket Number (provided by SITROOM):

INCIDENT INFORMATION
(Information regarding the individual (s) believed responsible for the PII incident)

Name of Individual(s) Believed Responsible for the PII Incident:
Position:
Address:
Company (Contractor) or **Region/Location** (Federal Staff):
Telephone No. - Office: **Telephone No. Cell**:
Name, Telephone Number and Email Address of the Individual's Supervisor (Security Officer for contract staff):
Location and Address of Incident (vehicle, hotel room, residence, etc.):
Incident Category (**must select from list**[2] **below**):
If category "Other" Selected, Briefly Describe:
Police Department (PD) Notifications (provide date/time, name of department and officer, and report number if available):
Description of PII Material Potentially Breached (Case Number(s)/Case Name(s)):
Date materials recovered or destroyed:
Details of recovery or destruction:
Summary of Incident: (Provide a detailed account of the incident include as many details as are known, history/timeline of events, number of cases lost, case numbers if known, what material was in case files, etc.):

[1] Times should be recorded in Eastern Time.
[2] Incident Category (Select Only One): Improper e-Access, Lost Shipment; Lost Laptop, Stolen Laptop, Lost Paper Files, Stolen Paper Files; Mis-sent Emails, Mis-sent Faxes; or other.

SUPERVISORY ACTIONS

(Identify All Actions Taken by Supervisor/Security Office)

Date/Time Notified:
Name of first line supervisor:
Date/time first line supervisor was notified:
Name of second line supervisor:
Date/time second line supervisor was notified:

Summary of Actions Taken By Supervisor/Security Office:

(NOTE: This input must be provided to the FIS Incident Response Team within 4 hours from the time of the initial report to the SITROOM)

INTERNAL USE ONLY

Date/Time Supervisor Input Received (if more than 4 hours, please explain):
FOIA/PA Branch Internal Tracking Number Assigned:
Entered Into PII Tracking System:
Date/Time FIS Incident Response Team Notified:
Incident Follow Up Assigned to:
Final Disposition:

EXHIBIT B

U.S. Office of Personnel Management
Federal Investigative Services

POLICY ON THE PROTECTION OF PERSONALLY IDENTIFIABLE INFORMATION (PII)

July 2014

Table of Contents

1.0 Introduction and Definitions

1.1 As an employee or contractor who works for or on behalf of the United States Office of Personnel Management (OPM), Federal Investigative Services (FIS), it is your responsibility to protect all personal information that has been entrusted to you. The Privacy Act of 1974 assigns this same personal individual responsibility to all Federal and Contract employees of all Federal Government Agencies. An essential component of meeting this responsibility is to ensure that you properly use, protect, and dispose of Personally Identifiable Information (PII).

The Privacy Act of 1974 also requires each agency to establish "Rules of Conduct": *Agencies are required to establish "rules of conduct for persons involved in the design, development, operation, or maintenance of any system of records, or in maintaining any record, and instruct each such person with respect to such rules and the requirements of [the Privacy Act], including any other rules and procedures adopted pursuant to [the Privacy Act] and the penalties for noncompliance." (5 U.S.C. § 552a(e)(9))*

1.2 As an Executive Agency within the United States Government, OPM has officially adopted the verbatim definition of PII established by the Office of Management and Budget (OMB) in 2007[1] and updated in 2010[2], which states: *The term "PII," as defined in OMB Memorandum M-07-16 refers to information that can be used to distinguish or trace an individual's identity, either alone or when combined with other personal or identifying information that is linked or linkable to a specific individual. The definition of PII is not anchored to any single category of information or technology. Rather, it requires a case-by-case assessment of the specific risk that an individual can be identified. In performing this assessment, it is important for an agency to recognize that non-PII can become PII whenever additional information is made publicly available — in any medium and from any source — that, when combined with other available information, could be used to identify an individual.*

The 2011 OPM Information Security & Privacy Policy Handbook[3] includes this definition on page 156, and it was re-affirmed by the OPM CIO in a memo issued to all OPM Program Offices on April 4, 2014 as the sole official OPM definition of PII to be used in all official documents, publications and contracts.

1.3 The following requirements are extracted directly from the OPM Information Security and Privacy Policy (ISPP) Addendum (FY12) March 2012[4], and apply to all OPM Federal and contract employees:

1.3.1 Scope and Applicability: The policies in this document, the same as the policies in the ISPP, apply to all OPM information resources. OPM information includes data that is owned, sent, received, or processed by the agency and includes information in either physical or digital form. OPM information resources include OPM hardware, software, media, and facilities. Everyone who uses,

1 http://www.whitehouse.gov/sites/default/files/omb/memoranda/fy2007/m07-16.pdf

2 http://www.whitehouse.gov/sites/default/files/omb/assets/memoranda_2010/m10-23.pdf

3 http://theo.opm.gov/policies/ispp/ISP_policy.pdf

4 http://theo.opm.gov/policies/ispp/P023PolicyAddendumMarch2012FINAL.pdf

manages, operates, maintains, or develops OPM applications or data wherever the applications or data reside must comply with the Information Security and Privacy Policy, unless a specific waiver is obtained from the Chief Information Officer (CIO) or the Chief Information Security Officer (CISO). The Information Security and Privacy Policy is also relevant to all contractors acting on behalf of OPM and to non-OPM organizations or their representatives who are granted authorized access to OPM information and information systems. Finally, this policy applies to other agencies' systems as delineated in Memorandums of Understanding (MOU) and Interconnection Security Agreements (ISA) with OPM.

1.3.2 Privacy Incident Response: The Federal Information Security Management Act (FISMA) requires that all Federal Agencies have a security program that includes procedures for detecting, reporting, and responding to security incidents. In compliance with FISMA, the Office of Personnel Management (OPM) has developed Agency-wide information security and privacy policies documented in the OPM Information Security and Privacy Policy Handbook that includes Incident Response (IR) policies. These addendum policies supplement the IR policies in the OPM ISPP, and are specific to Incidents involving PII.

OPM Employees / Contractors are responsible for:

- Capturing relevant information about the suspected or confirmed breach.
- Reporting any privacy incident or suspected privacy incident to their First-Line Supervisor immediately when becoming aware of the risk -regardless of the time or day of the week following the established reporting procedure. If supervisor is not available, employees are responsible for reporting to the Situation Room.

1.4 All OPM/FIS personnel and contractor personnel should limit the printing and transporting of PII whenever possible to minimize potential loss. The less hardcopy PII we have outside of our control, the more we reduce our vulnerability to a PII breach.

1.5 Chain of custody is defined as control of material pertaining to a Subject of an investigation upon receipt until PII is properly relinquished to an approved authority or properly destroyed.

1.6 OPM relinquishes responsibility in the chain of custody when it properly leaves our control and is successfully transmitted to an official authorized to use the PII in order to receive information or when transferred to another Federal Agency for adjudicative or informational purposes.

- Transfer of PII responsibility/accountability occurs only if the information has been positively confirmed to have been received by the intended gaining OPM/FIS office/facility or other authorized parties.

1.6.1 When it cannot be determined that PII sent to or between OPM/FIS facilities has been received at an OPM/FIS facility, it is the responsibility of the sending party to determine the disposition of the information (chain of custody status) and report any breach of PII through their respective chain of command.

2.0 Responsibilities

The OPM Chief Information Officer shall be responsible for establishing and maintaining the information security and privacy program at OPM and serves as the Chief Privacy Officer (also known as the OPM Senior Agency Official for Privacy).[5]

2.1 The Associate Director, FIS, is responsible for establishing policies and procedures that ensure the protection of all PII entrusted to OPM/FIS.

2.2 The Executive Program Director (EPD) of FIS Integrity Assurance is designated as the OPM/FIS Senior PII Representative and oversees the OPM/FIS PII Program on behalf of the Associate Director. In addition to establishing and updating OPM/FIS' PII Policy, the EPD of OPM/FIS Integrity Assurance is also responsible for overseeing the handling of PII incidents and recommending notification to victim(s) whose PII has been lost or otherwise compromised. Any changes or variations to the requirements of this policy must be approved by FIS' EPD for Integrity Assurance.

2.3 All FIS personnel and contractors are responsible for ensuring full compliance with all PII policies. FIS personnel and contractors must immediately report any possible compromise of PII following the established reporting procedures. Failure to adhere to PII Policy, to include reporting procedures, may be grounds for disciplinary or adverse action, up to and including removal.

3.0 Standards

3.1 OPM/FIS personnel, to include both Federal staff and contractors, are trusted with highly sensitive PII, the protection of which is an inherent responsibility of all personnel. OPM/FIS Standards for the protection of PII are based on the mandatory compliance requirements of Federal statutes, OMB Guidance, and OPM / FIS policies.

All PII entrusted to or controlled by OPM FIS federal or contract employees is further subject to and covered by the requirements of the specific OPM System of Records Notice (SORN) and OPM Privacy Impact Assessment that document the requirements and authorizations for any PII collected, maintained, or disclosed for the purposes for which specific OPM FIS systems are operated. The applicable SORNs are available from the OPM CISO office and establish requirements related to PII handling beyond protection that include sharing with other systems, retention schedules, specific encryption or handling requirements, and limits on uses of certain information.

While OPM/FIS will establish certain minimum standards of control, as defined throughout this document, OPM/FIS management recognizes the constantly changing nature and varying circumstances amongst most OPM/FIS staff, and therefore relies heavily upon its staff to exercise good judgment and to ensure compliance with all applicable requirements for protecting PII.

[5] [5] http://theo.opm.gov/policies/ispp/ISP_policy.pdf

3.1.1 This policy establishes minimum standards for the protection of PII. Supervisory personnel may establish stricter controls for the handling of PII based upon office location and circumstances unique to an individual area. Any additional controls placed upon individual personnel, as a result of specific circumstances, will be considered an enhancement to the mandatory minimum requirements outlined in this document.

3.1.2 FIS Personnel who have signed an individual telework agreement, which places additional measures of control, must adhere to the specific PII standards and policies within the individual telework agreement.

3.1.3 Any requests for variances from this policy must be submitted through supervisory channels. Upon approval of the supervisory chain, the request will be submitted to OPM/FIS Integrity Assurance for a final determination. All variances require approval of OPM/FIS Integrity Assurance prior to implementation.

3.2 OPM/FIS Field Office and Satellite Office storage requirements:

3.2.1 All case materials must be turned into the Field Offices for retention. Case materials may not be stored at Satellite Office or other locations beyond the 30 day requirement.

3.2.2 A two barrier rule applies to the protection of all PII within OPM/FIS and contractor office space.

3.2.3 The primary barrier in all OPM/FIS and contractor office space shall be a locked exterior office door, to prevent the entry of unauthorized individuals. All exterior locks must be changed within 7 days following a favorable termination (to include termination of office access) and within 24 hours of an unfavorable termination (or termination of office access).

3.2.4 During regular office hours, staff and office personnel may serve as the second barrier for the protection of unauthorized access to PII within FIS' control.

3.2.5 When an office is not staffed (i.e., outside of core hours or when authorized staff is out of the office), PII shall be secured within a locking file cabinet or within a designated storage area behind a separately locked internal door. A locked file cabinet or separately secured internal door will serve as the second barrier during times when an office is not staffed with OPM/FIS or contractor personnel.

3.2.6 Due to the unique nature and security policies of FIS core facilities at Boyers, Ft. Meade, and the Theodore Roosevelt Building, section 3.2.5 is not applicable to these locations, due to additional security measures already in place.

3.2.7 Individuals who are not properly cleared for authorized access to OPM/FIS office space must be escorted at all times.

3.3 Domicile storage requirements:

3.3.1 Information will be secured from access by others, including family members and guests, who may access the domicile location.

3.3.2 When the domicile location is unattended and contains PII the residence must be locked and adhere to the two barrier rule.

3.3.3 All personnel will provide their first line supervisor with documentation explaining how PII is stored and protected within their residence. Documentation will be provided within 30 days of receipt of this policy and subsequently updated within 30 days of any change in domicile storage procedures. First line supervisors will maintain current copies of each employee's submission and must obtain yearly updates from their staff. It is the responsibility of the supervisor to determine whether or not the submitted plan is acceptable.

3.4 Vehicle storage requirements:

3.4.1 Vehicles are used for the transport of PII between official locations, when such transport is required for conducting official FIS business. As such, PII will never be left in a vehicle overnight or for any other extended period of time. While it is recognized that the storage of PII in vehicles, under certain circumstances, will be unavoidable, whenever possible OPM/FIS personnel shall take PII with them and not leave it in a vehicle. While it is emphasized that only the minimum PII necessary to work productively should be carried into the field, it is recognized that some investigative activities, such as those conducted in residential areas, require that the investigator travel lightly. Under these limited circumstances, PII may be secured in a locked trunk, as long as the information is secured in a manner that complies with sections 3.4.2 through 3.4.6.

3.4.2 Case material will never be left unattended while in plain view or in any area other than the trunk of the vehicle.

3.4.3 The only authorized storage location for PII, within a parked vehicle, is within a locked trunk. When storing PII within a locked trunk, personnel shall take measures to place the PII in the trunk prior to arriving at their destination, so as to avoid drawing attention to the storage of materials within the trunk.

3.4.4 If the vehicle does not have a separate locking trunk area, as is such with certain sport utility vehicles, personnel will place the PII in the equivalent area of the vehicle and ensure it is covered from plain view and does not attract unusual attention.

3.4.5 Personnel will ensure the vehicle is locked and that all windows are fully closed, prior to leaving the vehicle.

3.4.6 Personnel will ensure items of value or other materials that may attract undue attention to a vehicle are secured and not within plain view (i.e., GPS units, cellular telephones, satellite radios, purses, packages, etc.).

3.5 Hotel room storage requirements:

3.5.1 Never leave material containing PII material in plain view, to include laptops.

3.5.2 If available, PII should be stored in a locked safe. If no locking safe is available, PII should be stored outside of plain view.

3.5.3 If unable to adequately secure PII within a hotel room, OPM/FIS personnel should evaluate if taking the material with them for temporary storage, to include within their vehicle, is more appropriate during times when not in the hotel room.

3.6 When traveling via airline or by other commercial means PII material, to include laptops or other information technology equipment containing PII, will never be stored within checked baggage and will remain within the control of the employee at all times.

3.7 When transporting PII between locations, it shall be contained within a closed container (i.e.: closed briefcase, zippered portfolio). PII shall not be transported in an open container, so as to reduce the potential for inadvertent loss.

4.0 PII Transmission Requirements

4.1 Upon receipt of case assignments, personnel are required to print necessary case material at their duty station, if equipped to do so. This replaces the shipment of case material by mail or other courier, whenever possible.

4.2 In the limited instance that case material is sent via the U.S. Postal Service (USPS) or other commercial carrier (e.g., UPS, FedEx, etc.), the material must be sent in such a method that allows for the item to be tracked throughout the entire shipping process. The use of a "delivery confirmation," in and of itself, will not suffice.

4.2.1 Any material sent via USPS or other commercial carrier will be fully manifested prior to sending. The manifest will contain the case names and associated numbers for all material contained within the shipment, along with any other relevant documents (i.e. releases, credit report, etc.) containing PII within the shipment. The sender of the shipment will include one copy of the manifest in the shipment and will retain a second copy, for use in the event of a lost or damaged shipment. All material will be double wrapped and sealed with the internal packaging also identifying the recipient of the information but without any markings indicating that PII is contained within the package. The internal envelope will have return address identification sticker in the event the exterior packaging is damaged.

4.2.2 Prior to sending any PII via USPS or other commercial carrier, the sender will notify the recipient of the shipment and its expected arrival date. Such notification shall be done via e-mail or other electronic method when possible.

4.2.3 Upon receipt of the shipment, the recipient (to include internal FIS shipments) will immediately reconcile the package contents with the enclosed manifest. Any discrepancies will be immediately reported to the sender and proper reporting requirements will be followed. Acknowledgement of the shipment shall be sent in the same manner in which the original notification of shipment was made. If the package does not arrive when expected, the recipient will notify the sender to initiate tracking of the package.

4.2.4 The shipper will retain the original manifest and recipient's confirmation for a period of two years. There is no requirement for the recipient to maintain a copy of the shipping manifest.

4.3 Transmission of PII via email:

4.3.1 Unsecure email is never to be used for transmission of PII or other case related material.

4.3.2 Messages sent to or from an e-mail address ending in "@OPM.GOV" are deemed secured. Messages sent to a recipient outside of the "OPM.GOV" domain must be encrypted for secure transmission. For these purposes only, the use of a Subject's last name and the case number will not be considered PII[6].

4.4 Thumb drive or other portable media storage of PII:

4.4.1 Thumb drives or other portable media may be used to store PII data provided the device is issued by OPM. PII placed on the device must be encrypted and must have the appropriate physical security controls in place.

4.5 Use of fax machines to transmit PII:

4.5.1 When faxing PII, the primary method for the transmission of PII should be a Government owned or controlled facsimile machine. When faxing material, FIS personnel should maintain visual control of the document(s) at all times. OPM/FIS Personnel and contractors will confirm the validity of fax numbers prior to sending.

4.5.2 The use of non-government or other commercial services for sending facsimiles (e.g.: FedEx Kinko's, Staples, OfficeMax, hotel business centers, etc.) is permitted when the sender is on TDY and does not have access to a government owned or controlled facsimile machine. In such instances, the sender will never relinquish visual control of the document and will insure accountability of the document at all times.

4.5.3 If receiving PII at a non-government or other commercial service facsimile, the recipient must be present at the time of transmission to receive the document. OPM/FIS personnel and contractors will never request a document containing PII be sent to a commercial service or other non-government location and have individuals unauthorized to view or handle FIS documents receive it for them (i.g, hotel staff, store employee, etc.).

4.5.4 OPM/FIS personnel and contractors will verify the receipt of all faxes. In cases where a machine generated delivery confirmation is available, this document shall be retained by personnel and will suffice as a delivery receipt. Personnel will store the confirmation receipt within the local case file; retention will be in accordance with current case retention policies.

[6] Reference April 3, 2014 e-mail from Chief Information Officer Services Bulletin regarding secure E-mail System Upgrade.

4.5.5 Frequently utilized numbers should be programmed into office and other government owned/issued facsimile machines in order to reduce the likelihood of error in sending facsimiles containing PII to unauthorized personnel/locations. Programmed numbers should be periodically checked to insure they are still valid.

4.6 Websites:

4.6.1 Entering PII (Subject identifiers such as name and SSN) on public internet sites to obtain investigative results is strictly prohibited unless specific authorization is received through appropriate procedures and the website has been authorized for such use by OPM/FIS.

4.6.2 Authorization regarding utilization of particular sites will be disseminated to personnel when the use of those sites has been approved by OPM/FIS.

4.6.3 Use of the internet is permissible for lead purposes. "Lead purposes" are those activities that may assist personnel in conducting investigations more efficiently and do not require inputting of PII for search results. Examples include locating addresses of facilities or phone numbers of individuals.

4.7 Completed cases:

4.7.1 Upon completion of fieldwork, field personnel will expeditiously return all completed materials and case notes to the originating field office. Under no circumstances will cases be held past the 7th day of the following month (i.e., cases completed in April, must be returned no later than May 7th).

4.7.2 Supervisors may require personnel to return case materials in a more expeditious manner than referenced in Section 4.7.1; under no circumstances will personnel hold cases for a longer period than defined in Section 4.7.1.

4.7.3 Unauthorized personnel will not destroy any case materials, including case notes, and must ensure all documents are returned to the field office for appropriate reconciliation and retention. Materials will be destroyed, by the first line supervisor or his/her designee, when directed to do so through case messaging. Personnel are not authorized to destroy case materials at their residences unless pre-approval is received.

4.7.4 Supervisors will ensure materials are properly destroyed within five business days of notification to do so. Personnel will maintain destruction logs of all case materials destroyed. Destruction logs will be maintained for a period of two years.

4.7.5 Investigative personnel will delete cases from their computer(s) within five business days of being directed to do so.

4.8 Releases:

4.8.1 When providing a release to a source, FIS personnel will redact the Date of birth and Social Security Number from the release.

5.0 Manifesting Requirements

5.1 The submission of a daily manifest to provide accountability of investigative case material in possession of personnel while moving between their duty stations and/or authorized locations is required.

5.2 Field personnel and/or teleworking employees will create and submit a manifest at the start of each working day, prior to transporting any PII. In cases where no PII is being transported, OPM/FIS personnel and contractors will submit a blank manifest or otherwise document to their supervisor that no PII will be transported that day. Documentation will be submitted daily, no later than 9 a.m. local time or prior to transporting any PII. A daily manifest is not required if an individual is not currently scheduled any items or cases; or, if the individual is a federal employee or direct employee of the prime contractor and is on leave or otherwise in a non-pay status. In such instances it will be the responsibility of the supervisor or the contractor's sub-contract manager to maintain documentation of an individual employee's or independent contractor's status.

5.2.1 Supervisory Agents-in-Charge (SAC's), first line supervisors, or sub-contract managers will ensure full accountability for daily manifests, as outlined above in 5.2.

5.3 Personnel with the need to transport material containing PII will be responsible for completing a detailed manifest. At a minimum, the manifest will contain the following information:

1. Date of manifest
2. Staff name
3. Case name (last), case number
4. Identification of the document(s) (case papers, release(s)/type of release(s), entire file)

5.4 Reconciliation of the manifest must be completed upon return to/arrival at the final duty location. Any discrepancies within the daily reconciliation of PII must be immediately reported as outlined in this policy.

5.4.1 Manifests will be maintained by supervisors for a period of two years from date of final receipt. Electronic storage of such manifests is acceptable.

5.5 Personnel who are in a TDY status will submit a daily manifest to both their assigned TDY supervisor and their home supervisor.

6.0 Reporting a Possible PII Breach

6.1 The determination about whether PII has been breached will be done carefully but promptly to ensure that the likelihood of a breach of PII is established by the preponderance of the data available. Mere suspicion of a breach should not be reported without further follow-up to determine the exact circumstances. To assist OPM/FIS personnel and contractors in assessing the likelihood of a PII breach, the following procedures shall be followed.

6.2 In evaluating whether or not to report a breach, FIS personnel shall consider all relevant factors. Instances of theft or any other immediately known loss should be reported as such. Cases of missing packages within the USPS or other commercial carrier should be investigated further to determine the likelihood of a lost package, as opposed to one that is simply delayed. In all instances, once a loss or other breach is suspected or known, it must be immediately reported.

6.2.1 Shipments that are confirmed to have been lost or cannot be accounted for after a reasonable period of time shall be reported as lost PII.

6.2.2 Misdirected faxes and other dissemination of documents to unauthorized individuals will be reported as lost PII.

6.2.3 In cases where it is undetermined whether or not an incident should be reported, personnel shall immediately contact the EPD of OPM/FIS Integrity Assurance for further guidance and instructions.

6.2.4 The responsibility for proper follow-up and additional measures regarding the investigation and/or recovery of lost materials will be that of the first line supervisor.

6.3 Notification:

6.3.1 Immediately upon becoming aware of a possible PII incident, the supervisor of the individual responsible for the loss will contact the OPM Situation Room (SITROOM). The SITROOM is available 24 hours per day, 7 days per week. The SITROOM will be notified either telephonically at (202) 418-0111 or via email at usopmsr@opm.gov. The reporting individual will provide all known details to the SITROOM. When reporting a PII breach it must be noted if National Agency Check (NAC) items are lost for proper reporting to the originating agency.

6.3.2 When reporting a breach, the SITROOM requires information to include name, location, number of cases, and as many details of the incident as possible. Specific PII of individuals should not be included (i.e. SSN).

6.3.3 Within four (4) hours from the point that the incident is reported to the SITROOM, the Supervisor of the individual believed responsible for the PII loss will coordinate with their supervisor (the second line supervisor for the employee who is believed responsible for the loss). In coordination, the individual responsible for the loss and their supervisor(s) will submit the FIS PII Loss Reporting Form to the FIS Incident Response Team, via email at FISINCIDENTRESPONSETEAM@OPM.GOV.

6.3.4 The responsible individual's Supervisor will take immediate steps to initiate recovery of the material and/or to follow up with additional parties relevant to the loss and/or recovery of PII material.

6.3.5 Supervisors are responsible for ensuring that the FIS Incident Response Team is immediately updated on changes to initially reported information (i.e., PII is found, lost shipment recovered, etc.).

6.3.6 If, within 60 days after the PII loss was initially reported, the status of the PII loss has not changed, or it has not been previously updated as per 6.3.4, the supervisor will provide a status update to FIS Integrity Assurance.

7.0 Official Loss Notifications

7.1 FIS Integrity Assurance will review each reported PII loss and make a recommendation to the FIS Freedom of Information and Privacy Act Office (FOIPA). FIS FOIPA will notify OPM OGC regarding appropriate notifications. FIS' Freedom of Information and Privacy Act Office will ensure all required notifications to the affected Subject(s) are made within three days of determination, unless specific circumstances of an individual loss dictate faster notification. All notifications will conform to the required internal procedures for such.

7.2 All notifications to Subject's affected by lost PII will be made as approved by the required procedures for such. Personnel not associated with the official notification procedures should not notify or otherwise inform the affected Subject(s) of lost PII. Any exceptions must be coordinated through OPM FIS Integrity Assurance and/or FIS' Freedom of Information and Privacy Act Office.

8.0 Compliance

8.1 FIS Integrity Assurance is responsible for oversight and ensuring full compliance with the established FIS PII Policy. To ensure compliance, FIS Integrity Assurance will conduct random audits of FIS offices. All personnel must fully comply with PII Audits.

8.2 Exceptions to the standards set forth in this policy will be submitted to FIS Integrity Assurance for review and determination. No exceptions are authorized without the prior approval of FIS Integrity Assurance.

8.3 Failure to follow the FIS PII Policy may result in disciplinary action, up to and including removal.

(Attachment 1)

ACKNOWLEDGEMENT OF RECEIPT

FIS Policy on the Protection of Personally Identifiable Information (PII), July 2014

I, _____ acknowledge receipt of the **FIS Policy on the Protection of Personally Identifiable Information (PII), July 2014**. I also understand that as a FIS employee or Contractor I am responsible for reviewing this document and discussing any questions or concerns with my supervisor.

_____ _____

Signature of Individual Date

THIS FORM IS TO BE RETAINED BY THE SUPERVISOR AND TRANSFERRED WITH THE EMPLOYEE AS NECESSARY.

(ATTACHMENT 2)

U.S. Office of Personnel Management
Federal Investigative Services

FIS PII LOSS REPORTING FORM
INITIAL NOTIFICATION

REPORTING INDIVIDUAL INFORMATION
(Information regarding individual discovering the PII incident)

Name of Reporting Individual:
Address:
Company (Contractor) or **Region** (Federal):
Telephone No.-Office: **Telephone No.-Cell**:
Email:
Date/Time [1] **the PII Incident Occurred (if known)**:
Ticket Number (provided by SITROOM):

INCIDENT INFORMATION
(Information regarding the individual (s) believed responsible for the PII incident)

Name of Individual(s) Believed Responsible for the PII Incident:
Position:
Address:
Company (Contractor) or **Region/Location** (Federal Staff):
Telephone No. - Office: **Telephone No. Cell**:
Name, Telephone Number and Email Address of the Individual's Supervisor (Security Officer for contract staff):
Location and Address of Incident (vehicle, hotel room, residence, etc.):
Incident Category (**must select from list**[2] **below**):
If category "Other" Selected, Briefly Describe:
Police Department (PD) Notifications (provide date/time, name of department and officer, and report number if available):
Description of PII Material Potentially Breached (Case Number(s)/Case Name(s)/material(s) lost (i.e.) case papers, releases, notes, etc.):
Date materials recovered or destroyed:
Details of recovery or destruction:
Summary of Incident: (Provide a detailed account of the incident include as many details as are known, history/timeline of events, number of cases lost, case numbers if known, what material was in case files, etc.):

[1] Times should be recorded in Eastern Time.
[2] Incident Category (Select Only One): Improper e-Access, Lost Shipment; Lost Laptop, Stolen Laptop, Lost Paper Files, Stolen Paper Files; Mis-sent Emails, Mis-sent Faxes; or other.

SUPERVISORY ACTIONS
(Identify All Actions Taken by Supervisor/Security Office)

JULY 2014 Edition – All Previous Editions Are Obsolete

Name of first line supervisor:
Date/time first line supervisor was notified:
Name of second line supervisor:
Date/time second line supervisor was notified:

Summary of Actions Taken By Supervisor/Security Office:

(NOTE: This input must be provided to the FIS Incident Response Team within 4 hours from the time of the initial report to the SITROOM)

INTERNAL USE ONLY

Date/Time Supervisor Input Received (if more than 4 hours, please explain):
FOIA/PA Branch Internal Tracking Number Assigned:
Entered Into PII Tracking System:
Date/Time FIS Incident Response Team Notified:
Incident Follow Up Assigned to:
Final Disposition:

U.S. OFFICE OF PERSONNEL MANAGEMENT

LATEST NEWS NEWS

Share

News Release

FOR IMMEDIATE RELEASE
Thursday, June 04, 2015
Contact: Sam Schumach
Tel: (202) 606-2402

OPM to Notify Employees of Cybersecurity Incident

WASHINGTON, DC – The U.S. Office of Personnel Management (OPM) has identified a cybersecurity incident potentially affecting personnel data for current and former federal employees, including personally identifiable information (PII).

Within the last year, the OPM has undertaken an aggressive effort to update its cybersecurity posture, adding numerous tools and capabilities to its networks. As a result, in April 2015, OPM detected a cyber-intrusion affecting its information technology (IT) systems and data. The intrusion predated the adoption of the tougher security controls.

OPM has partnered with the U.S. Department of Homeland Security's Computer Emergency Readiness Team (US-CERT) and the Federal Bureau of Investigation (FBI) to determine the full impact to Federal personnel. OPM continues to improve security for the sensitive information it manages and evaluates its IT security protocols on a continuous basis to protect sensitive data to the greatest extent possible. Since the intrusion, OPM has instituted additional network security precautions, including: restricting remote access for network administrators and restricting network administration functions remotely; a review of all connections to ensure that only legitimate business connections have access to the internet; and deploying anti-malware software across the environment to protect and prevent the deployment or execution of tools that could compromise the network.

As a result of the incident, OPM will send notifications to approximately 4 million individuals whose PII may have been compromised. Since the investigation is on-going, additional PII exposures may come to light; in that case, OPM will conduct additional notifications as necessary. In order to mitigate the risk of fraud and identity theft, OPM is offering credit report access, credit monitoring and identify theft insurance and recovery services to potentially affected individuals through CSID®, a company that specializes in these services. This comprehensive, 18-month membership includes credit monitoring and $1 million in identity theft protection services at no cost to enrollees.

"Protecting our Federal employee data from malicious cyber incidents is of the highest priority at OPM," said **OPM Director Katherine Archuleta**. "We take very seriously our responsibility to secure the information stored in our systems, and in coordination with our agency partners, our experienced team is constantly identifying opportunities to further protect the data with which we are entrusted."

OPM has issued the following guidance to affected individuals:

- Monitor financial account statements and immediately report any suspicious or unusual activity to financial institutions.
- Request a free credit report at www.AnnualCreditReport.com or by calling 1-877-322-8228. Consumers are entitled by law to one free credit report per year from each of the three major credit bureaus – Equifax®, Experian®, and TransUnion® – for a total of three reports every year. Contact information for the credit bureaus can be found on the Federal Trade Commission (FTC) website, www.ftc.gov.
- Review resources provided on the FTC identity theft website, www.identitytheft.gov. The FTC maintains a variety of consumer publications providing comprehensive information on computer intrusions and identity theft.
- You may place a fraud alert on your credit file to let creditors know to contact you before opening a new account in your name. Simply call TransUnion® at 1-800-680-7289 to place this alert. TransUnion® will then notify the other two credit bureaus on your behalf.

How to avoid being a victim:

- Be suspicious of unsolicited phone calls, visits, or email messages from individuals asking about employees or other internal information. If an unknown individual claims to be from a legitimate organization, try to verify his or her identity directly with the company.
- Do not provide personal information or information about your organization, including its structure or networks, unless you are certain of a person's authority to have the information.
- Do not reveal personal or financial information in email, and do not respond to email solicitations for this information. This includes following links sent in email.
- Do not send sensitive information over the Internet before checking a website's security (for more information, see Protecting Your Privacy, http://www.us-cert.gov/ncas/tips/ST04-013).
- Pay attention to the URL of a website. Malicious websites may look identical to a legitimate site, but the URL may use a variation in spelling or a different domain (e.g., .com vs. .net).
- If you are unsure whether an email request is legitimate, try to verify it by contacting the company directly. Do not use contact information provided on a website connected to the request; instead, check previous statements for contact information. Information about known phishing attacks is also available online from groups such as the Anti-Phishing Working Group (http://www.antiphishing.org).
- Install and maintain anti-virus software, firewalls, and email filters to reduce some of this traffic (for more information, see Understanding Firewalls, http://www.us-cert.gov/ncas/tips/ST04-004; Understanding Anti-Virus Software, http://www.us-cert.gov/ncas/tips/ST04-005; and Reducing Spam, http://www.us-cert.gov/ncas/tips/ST04-007).

- Take advantage of any anti-phishing features offered by your email client and web browser.
- Employees should take steps to monitor their personally identifiable information and report any suspected instances of identity theft to the FBI's Internet Crime Complaint Center at www.ic3.gov.

Potentially affected individuals can obtain additional information about the steps they can take to avoid identity theft from the following agencies. The FTC also encourages those who discover that their information has been misused to file a complaint with them.

For California Residents: Visit the California Office of Privacy Protection (www.privacy.ca.gov) for additional information on protection against identity theft	**For Kentucky Residents:** Office of the Attorney General of Kentucky 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601 www.ag.ky.gov Telephone: 1-502-696-5300
For Maryland Residents: Office of the Attorney General of Maryland Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202 www.oag.state.md.us/Consumer Telephone: 1-888-743-0023	**For North Carolina Residents:** Office of the Attorney General of North Carolina 9001 Mail Service Center Raleigh, NC 27699-9001 www.ncdoj.com/ Telephone: 1-919-716-6400
For all other US Residents: Identity Theft Clearinghouse Federal Trade Commission	

600 Pennsylvania Avenue, NW

Washington, DC 20580

www.identitytheft.gov

1-877-IDTHEFT (438-4338)

TDD: 1-202-326-2502

- end -

Our mission is to Recruit, Retain and Honor a World-Class Workforce to Serve the American People. OPM supports U.S. agencies with personnel services and policy leadership including staffing tools, guidance on labor-management relations and programs to improve work force performance.

Tel: 202-606-2402 | Fax: 202-606-2264

U.S. OFFICE OF PERSONNEL MANAGEMENT

LATEST NEWS NEWS

Share

News Release

FOR IMMEDIATE RELEASE
Thursday, July 09, 2015
Contact: Office of Communications
Tel: 202-606-2402

OPM Announces Steps to Protect Federal Workers and Others From Cyber Threats

WASHINGTON, D.C. – Today, the U.S. Office of Personnel Management (OPM) announced the results of the interagency forensics investigation into a recent cyber incident involving Federal background investigation data and the steps it is taking to protect those impacted. Throughout this investigation, OPM has been committed to providing information in a timely, transparent and accurate manner. As information has become available and verifiable, the agency has updated Congress, the Inspector General, Federal employee representatives, and – most importantly – those that are affected. Today's announcement is the latest in this series of updates, and OPM will continue to provide additional information going forward.

Background on the intrusion into OPM's systems. Since the end of 2013, OPM has undertaken an aggressive effort to upgrade the agency's cybersecurity posture, adding numerous tools and capabilities to its various legacy networks. As a direct result of these steps, OPM was able to identify two separate but related cybersecurity incidents on its systems.

Today, OPM announced the results of the interagency forensic investigation into the second incident. As previously announced, in late-May 2015, as a result of ongoing efforts to secure its systems, OPM discovered an incident affecting **background investigation records** of current, former, and prospective Federal employees and contractors. Following the conclusion of the forensics investigation, OPM has determined that the types of information in these records include identification details such as Social Security Numbers; residency and educational history; employment history; information about immediate family and other personal and business acquaintances; health, criminal and financial history; and other details. Some records also include findings from interviews conducted by background investigators and fingerprints. Usernames and passwords that background investigation applicants used to fill out their background investigation forms were also stolen.

While background investigation records do contain some information regarding mental health and financial history provided by those that have applied for a security clearance and by individuals

contacted during the background investigation, there is no evidence that separate systems that store information regarding the health, financial, payroll and retirement records of Federal personnel were impacted by this incident (for example, annuity rolls, retirement records, USA JOBS, Employee Express).

This incident is separate but related to a previous incident, discovered in April 2015, affecting **personnel data** for current and former Federal employees. OPM and its interagency partners concluded with a high degree of confidence that personnel data for 4.2 million individuals had been stolen. This number has not changed since it was announced by OPM in early June, and OPM has worked to notify all of these individuals and ensure that they are provided with the appropriate support and tools to protect their personal information.

Analysis of background investigation incident. Since learning of the incident affecting background investigation records, OPM and the interagency incident response team have moved swiftly and thoroughly to assess the breach, analyze what data may have been stolen, and identify those individuals who may be affected. The team has now concluded with high confidence that sensitive information, including the Social Security Numbers (SSNs) of 21.5 million individuals, was stolen from the background investigation databases. This includes 19.7 million individuals that applied for a background investigation, and 1.8 million non-applicants, predominantly spouses or co-habitants of applicants. As noted above, some records also include findings from interviews conducted by background investigators and approximately 1.1 million include fingerprints. There is no information at this time to suggest any misuse or further dissemination of the information that was stolen from OPM's systems.

If an individual underwent a background investigation through OPM in 2000 or afterwards (which occurs through the submission of forms SF 86, SF 85, or SF 85P for a new investigation or periodic reinvestigation), it is highly likely that the individual is impacted by this cyber breach. If an individual underwent a background investigation prior to 2000, that individual still may be impacted, but it is less likely.

Assistance for impacted individuals. OPM is also announcing the steps it is taking to protect those impacted:

1. Providing a comprehensive suite of monitoring and protection services for background investigation applicants and non-applicants whose Social Security Numbers, and in many cases other sensitive information, were stolen – For the 21.5 million background investigation applicants, spouses or co-habitants with Social Security Numbers and other sensitive information that was stolen from OPM databases, OPM and the Department of Defense (DOD) will work with a private-sector firm specializing in credit and identity theft monitoring to provide services such as:

- Full service identity restoration support and victim recovery assistance
- Identity theft insurance
- Identity monitoring for minor children
- Continuous credit monitoring
- Fraud monitoring services beyond credit files

The protections in this suite of services are tailored to address potential risks created by this particular incident, and will be provided for a period of at least 3 years, at no charge.

In the coming weeks, OPM will begin to send notification packages to these individuals, which will provide details on the incident and information on how to access these services. OPM will also provide educational materials and guidance to help them prevent identity theft, better secure their personal and work-related data, and become more generally informed about cyber threats and other risks presented by malicious actors.

2. Helping other individuals who had other information included on background investigation forms – Beyond background investigation applicants and their spouses or co-habitants described above, there are other individuals whose name, address, date of birth, or other similar information may have been listed on a background investigation form, but whose Social Security Numbers are not included. These individuals could include immediate family members or other close contacts of the applicant. In many cases, the information about these individuals is the same as information generally available in public forums, such as online directories or social media, and therefore the compromise of this information generally does not present the same level of risk of identity theft or other issues.

The notification package that will be sent to background investigation applicants will include detailed information that the applicant can provide to individuals he or she may have listed on a background investigation form. This information will explain the types of data that may have been included on the form, best practices they can exercise to protect themselves, and the resources publicly available to address questions or concerns.

3. Establishing an online cybersecurity incident resource center – Today, OPM launched a new, online incident resource center - located at https://www.opm.gov/cybersecurity - to offer information regarding the OPM incidents as well as direct individuals to materials, training, and useful information on best practices to secure data, protect against identity theft, and stay safe online. This resource site will be regularly updated with the most recent information about both the personnel records and background investigation incidents, responses to frequently asked questions, and tools that can help guard against emerging cyber threats.

4. Establishing a call center to respond to questions – In the coming weeks, a call center will be opened to respond to questions and provide more information. In the interim, individuals are encouraged to visit https://www.opm.gov/cybersecurity. Individuals will not be able to receive personalized information until notifications begin and the call center is opened. OPM recognizes that it is important to be able to provide individual assistance to those that reach out with questions, and will work with its partners to establish this call center as quickly as possible.

5. Protecting all Federal employees – In the coming months, the Administration will work with Federal employee representatives and other stakeholders to develop a proposal for the types of credit and identity theft monitoring services that should be provided to all Federal employees in the future – regardless of whether they have been affected by this incident – to ensure their personal information is always protected.

Continuing to strengthen OPM cybersecurity. OPM continues to take aggressive action to strengthen its broader cyber defenses and information technology (IT) systems, in partnership with experts from DOD, the Department of Homeland Security, the Federal Bureau of Investigation, and its other interagency partners. As outlined in its recent Cybersecurity Action Report, in June, OPM identified 15 new steps to improve security, leverage outside expertise, modernize its systems, and ensure internal accountability in its cyber practices. This includes completing deployment of two-factor Strong Authentication for all users, expanding continuous monitoring of its systems, and hiring a new cybersecurity advisor.

Director Archuleta has initiated a comprehensive review of the architectural design of OPM's IT systems, to identify and immediately mitigate any other vulnerabilities that may exist, and assess OPM's data sharing and use policies. That review is ongoing. In addition, OPM will also continue to participate in a Federal Government-wide 30-day cybersecurity sprint, whereby immediate steps are being taken to further protect information and assets and improve the resilience of Federal networks, and will participate in a 90-day interagency review of key questions related to information security, governance, policy, and other aspects of this the security and suitability determination process, to ensure that it is conducted in the most efficient, effective and secure manner possible.

Director Archuleta and the entire Office of Personnel Management are committed to protecting the safety and security of the information of Federal employees and contractors. OPM is also committed to helping those that have been impacted by this incident, safeguarding its systems and data, and fulfilling its mission to serve Federal workers.

- end -

Our mission is to Recruit, Retain and Honor a World-Class Workforce to Serve the American People. OPM supports U.S. agencies with personnel services and policy leadership including staffing tools, guidance on labor-management relations and programs to improve work force performance.

Tel: 202-606-2402 | Fax: 202-606-2264

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN RE U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION	Misc. Action No. 15-1394 (ABJ) MDL Docket No. 2664
This Document Relates To: *NTEU v. Cobert*, 15-cv-1808-ABJ (D.D.C.) 3:15-cv-03144 (N.D. Cal.)	**AMENDED COMPLAINT FOR DECLARATORY AND INJUNCTIVE RELIEF**

INTRODUCTION

This action seeks a remedy for the unconstitutional disclosure by the federal government of the personal information of members of the National Treasury Employees Union (NTEU) currently or formerly employed by the federal government. When the government collected the information in question, it assured the individuals who provided the information that it would be safeguarded and kept confidential. On June 4, 2015, the Office of Personnel Management (OPM) announced that it had become aware of a breach in its data systems, which resulted in unauthorized access to the personal information of 4.2 million current and former federal employees, including numerous NTEU members. According to OPM, the types of information that may have been compromised include name, Social Security number, date and place of birth, and current and former addresses. OPM

notified thousands of NTEU members that their personal information was compromised by this data breach.

OPM cautioned that, as its investigation continued, additional exposure could be discovered. On June 12, 2015, OPM announced that it had experienced another breach, which it later confirmed implicated the personal information of 21.5 million individuals. This breach resulted in unauthorized access to data systems containing materials related to the background investigations of current, former, and prospective federal employees. OPM notified thousands of NTEU members that their personal information was compromised by this data breach.

Among the materials compromised in the breach announced on June 12, 2015, were an unknown number of completed Standard Form 86's (SF-86). The SF-86 (Questionnaire for National Security Positions) is a form that individuals complete in order to be considered for or retained in national security positions as defined in 5 C.F.R. Part 732 and to obtain access to classified information under Executive Order 12968.

Because the breach announced on June 12, 2015 involved background investigation materials, the compromised materials also included an unknown number of completed Standard Form 85's (SF-85) and Standard Form 85P's (SF-85P). The SF-85 (Questionnaire for Non-Sensitive Positions) is a form that individuals complete as part of a background investigation to determine whether they, as applicants or incumbents, are suitable for federal employment. The SF-85P (Questionnaire for Public Trust Positions) is a form that individuals complete as

part of background investigations to determine whether they, as applicants or incumbents, are suitable for federal employment in "public trust" or "sensitive" positions, as defined in 5 C.F.R. Part 731. Completed SF-85's, SF-85P's, and SF-86's contain personal information relating to the individual completing the form and to that person's relatives, friends, and others.

These massive data breaches came after OPM had been put on notice of deficiencies in its information security practices by OPM's Office of Inspector General (OIG). Over a period of many years, the OIG had identified numerous significant deficiencies, including deficiencies related to OPM's decentralized security governance structure, its failure to ensure that its information technology systems met applicable security standards, and its failure to ensure that adequate technical security controls were in place for all servers and databases.

Although on notice of serious flaws in its data system security, OPM failed to adequately secure personal information in its possession -- a failure that was reckless under the circumstances. OPM's reckless failure to safeguard personal information to which it had been entrusted resulted in the unauthorized disclosure of NTEU members' personal information in violation of their right, under the U.S. Constitution, including the Due Process Clause of the Fifth Amendment, to informational privacy. Plaintiffs seek a declaration that OPM's conduct was unconstitutional and other equitable relief.

JURISDICTION

1. This Court has jurisdiction pursuant to 28 U.S.C. § 1331.

VENUE

2. This lawsuit was originally filed in the Northern District of California before being transferred for coordinated or consolidated pretrial proceedings to this District. Plaintiffs have not waived—and, by the filing of this amended complaint, do not waive—their rights under Lexecon Inc. v. Milberg Weiss Bershad Hynes & Lerach, 523 U.S. 26 (1998), and 28 U.S.C. § 1407(a), to seek a remand to the Northern District of California at the conclusion of pretrial proceedings. Thus, Plaintiffs, here, allege that venue is proper in the Northern District of California and also proper in this District.

3. Venue is proper in the Northern District of California pursuant to 28 U.S.C. § 1391(e). Venue is proper in the San Francisco-Oakland Division under Local Rule 3-2 because NTEU has a field office in Oakland, California, and has many members who reside or work within the Division who were affected by the OPM data breaches described in this complaint; Plaintiffs Stephen Howell and Jonathon Ortino reside within the Division; and Plaintiff Ortino works within the Division. Thus, Plaintiffs Howell and Ortino's respective injuries have occurred, at least in substantial part, within the Division.

4. Venue is also proper in this District pursuant to 28 U.S.C. § 1391(e) because Defendant, Beth Cobert, Acting Director of the Office of Personnel Management, in her official capacity, resides in the District of Columbia.

PARTIES

5. Plaintiff NTEU is an unincorporated association with its principal place of business at 1750 H Street, N.W., Washington, D.C. 20006. Pursuant to Title VII of the Civil Service Reform Act, Public Law No. 95-454, 92 Stat. 1111, NTEU is the exclusive bargaining representative of approximately 150,000 federal employees in 31 federal agencies, including thousands of dues-paying members whose personal information has been compromised. NTEU represents the interests of these employees by, inter alia, negotiating collective bargaining agreements; arbitrating grievances under such agreements; filing unfair labor practices; lobbying Congress for favorable working conditions, pay, and benefits; and enforcing employees' collective and individual rights in federal courts. NTEU brings this action in its representative capacity on behalf of its members who have been injured by the Defendant's failure to protect their personal information.

6. Plaintiff Eugene Gambardella resides in Manalapan, NJ. He is employed by Customs and Border Protection (CBP) in Newark, NJ, as a Senior Import Specialist. He is a member of a bargaining unit for which NTEU is the exclusive representative and is a dues-paying member of NTEU. Mr. Gambardella submitted an SF-85P when he was hired by CBP, and later submitted an SF-86 to CBP during a standard reinvestigation. Through these forms, he disclosed or authorized the release to OPM of, among other information, medical information (including mental health information), financial information (including his investment accounts), marital information, nonpublic information about his family

(including the citizenship papers, immigration numbers, and passport numbers of relatives), and his Social Security Number.

7. Plaintiff Stephen Howell resides in Pleasanton, CA (Alameda County). He is employed by the Internal Revenue Service (IRS) in San Jose, CA, as an Appeals Officer. He is a member of a bargaining unit for which NTEU is the exclusive representative and is a dues-paying member of NTEU. Mr. Howell submitted an SF-86 when he was hired by IRS, disclosing or authorizing the release to OPM of, among other information, medical information (including mental health information), marital information, nonpublic information about his family, and his Social Security Number.

8. Plaintiff Jonathon Ortino resides in Burlingame, CA (San Mateo County). He is employed by CBP in San Francisco, CA, as a Customs and Border Protection Officer. He is a member of a bargaining unit for which NTEU is the exclusive representative and is a dues-paying member of NTEU. Mr. Ortino submitted an SF-86 when he was hired by CBP, disclosing or authorizing the release to OPM of, among other information, medical information (including mental health information), financial information, marital information, nonpublic information about his family, and his Social Security Number. Mr. Ortino was subject to a periodic reinvestigation in 2012.

9. Defendant Beth F. Cobert is Acting Director of OPM. Acting Director Cobert succeeded former Director of OPM Katherine Archuleta, who resigned as Director in the wake of the data breaches described in this amended complaint. As

Acting Director, Ms. Cobert is responsible for executing, administering, and enforcing civil service laws and regulations, including the requirement that federal government applicants and employees undergo background investigations. She is also responsible for ensuring that personal information entrusted to OPM is protected from unauthorized disclosure. The Acting Director is sued solely in her official capacity.

STATEMENT OF CLAIMS

OPM's Data Collection and Retention

10. In its role as the federal civil service's personnel manager, OPM collects and stores immense amounts of federal employee data. It manages a software system that provides internet-based access to employee personnel folders. That system is called the electronic Official Personnel Folder (eOPF), and its contents include employee performance records, employment history, benefits, job applications, resumes, education transcripts, and birth certificates.

11. OPM conducts over two million background investigations a year. These investigations, which are required by Executive Orders and other rules and regulations, are used by the federal government to make suitability and security clearance determinations.

12. OPM uses a variety of database systems as part of its investigative function, including those discussed in this paragraph. It uses a web-based automated software system to process standard investigative forms used for background investigations: the Electronic Questionnaires for Investigations

Processing (e-QIP). eQIP is intended to allow for the secure transmission of personal investigative data to the requesting agency. OPM's Personal Investigations Processing System (PIPS) is a background investigation software system that handles individual investigation requests from agencies. It contains an index of background investigations conducted on federal employees. OPM's Central Verification System (CVS) contains information on security clearances, investigations, suitability determinations, background checks for those seeking access to federal facilities, and polygraph data.

The Breach Announced on June 4, 2015

13. OPM experienced a cybersecurity incident, which it announced on June 4, 2015, that compromised the personal information of 4.2 million individuals. OPM sent letters to those affected by the incident to notify them that their personal information was compromised.

14. OPM first detected the incident in April 2015. See News Release, OPM to Notify Employees of Cybersecurity Incident, Office of Personnel Management (June 4, 2015). This cybersecurity incident is believed to have been perpetrated in October 2014. See Sean Lyngaas, Exclusive: The OPM Breach Details That You Haven't Seen, Federal Computer World (Aug. 21, 2015), available at https://fcw.com/articles/2015/08/21/opm-breach-timeline.aspx (drawing upon timeline for OPM cybersecurity incidents provided in July 14, 2015 document "prepared by federal investigators for the office of U.S. CIO Tony Scott"). During

this time, the perpetrators of the cybersecurity incident accessed and took personal information housed in the accessed OPM data systems, as detailed below.

15. On or about June 9, 2015, OPM posted on its website a set of "Frequently Asked Questions" (FAQ) that included information about this data breach. One of the FAQ's read as follows:

> What personal information was compromised
>
> OPM maintains personnel records for the Federal workforce. The kind of data that may have been compromised in this incident could include name, Social Security Number, date and place of birth, and current and former addresses. It is the type of information you would typically find in a personnel file, such as job assignments, training records, and benefit selection decisions, but not the names of family members or beneficiaries and not information contained in actual policies. The notifications to potentially affected individuals will state exactly what information may have been compromised.

16. Thousands of NTEU members were determined by OPM to have been affected by this first data breach and have received the notification described in Paragraphs 13 and 15. Those NTEU members, including Plaintiffs Gambardella, Howell, and Ortino, were subject to unauthorized access of their personal information through the breach, and the taking of that information.

17. After discovering the intrusion that it announced on June 4, 2015, OPM publicly stated that, since its investigation was ongoing, additional exposures of personal information could be discovered.

The Breach Announced on June 12, 2015

18. On June 12, 2015, OPM announced a second data breach. OPM first detected the incident in May 2015. See News Release, OPM Announces Steps to

Protect Federal Workers and Others From Cyber Threats, Office of Personnel Management (July 9, 2015). This data breach is believed to have been perpetrated in July and August 2014. See Sean Lyngaas, Exclusive: The OPM Breach Details That You Haven't Seen, Federal Computer World (Aug. 21, 2015), available at, https://fcw.com/articles/2015/08/21/opm-breach-timeline.aspx (referencing timeline for OPM cyber incidents provided in July 14, 2015, document "prepared by federal investigators for the office of U.S. CIO Tony Scott"). During this time, the perpetrators of the data breach accessed and took personal information housed in the accessed OPM data systems, as detailed below.

19. Based on OPM's public announcements, this data breach involved OPM systems, such as those discussed in Paragraph 12, containing, among other information, information related to the background investigations of current, former, and prospective federal government employees. In all, this breach compromised the personal information of 21.5 million individuals. OPM would later announce, on September 23, 2015, that the perpetrators of the breach accessed and took the fingerprints of approximately 5.6 million current, former, and prospective federal government employees. OPM has sent letters to those affected by this breach. NTEU members who underwent federal background investigations were subject to unauthorized access of their background investigation information through the breach, and the taking of that information.

20. As part of the background investigations described in Paragraph 11, federal employees and applicants are required to submit forms such as the

Standard Form 85 (Questionnaire for Non-Sensitive Positions) (SF-85); Standard Form 85P (Questionnaire for Public Trust Positions) (SF-85P); and Standard Form 86 (Questionnaire for National Security Positions) (SF-86).

21. A completed, current version of the SF-85 (Form Approved OMB No. 3206-0261) can contain, inter alia, the following information about the individual who has completed it: Social Security number; citizenship; prior addresses; education; employment history; information about persons who know the individual well; selective service record; military history; and whether the individual has used, possessed, supplied, or manufactured illegal drugs.

22. The current version of the SF-85 includes an "Authorization for Release of Information" to authorize background investigators "to obtain any information relating to [the individual's] activities from individuals, schools, residential management agents, employers, criminal justice agencies, credit bureaus, consumer reporting agencies, retail business establishments, or other sources of information to include publically available electronic information. This information may include, but is not limited to, [the individual's] academic, residential, achievement, performance, attendance, disciplinary, employment history, and criminal history record information."

23. Including instructions, the current online version of the SF-85 is eight pages in length.

24. In addition to information contained on the SF-85, a completed, current version of the SF-85P (Form Approved OMB No. 3206-0191) can also

include marital status information; information about relatives; information about previous background investigations; foreign countries visited; police record; and financial history.

25. The current version of the SF-85P includes an "Authorization for Release of Information" similar in its coverage to that included in the SF-85, except that the SF-85P release also allows investigators to collect financial and credit information.

26. The current version of the SF-85P includes an "Authorization for Release of Medical Information" that, when signed, permits an investigator to ask the individual's health care practitioner the following three questions about the individual's mental health:

> Does the person under investigation have a condition or treatment that could impair his/her judgment or reliability?
>
> If so, please describe the nature of the condition and the extent and duration of the impairment or treatment.
>
> What is the prognosis?

27. The current version of the SF-85P includes a "Supplemental Questionnaire for Selected Positions" with additional questions about the use of illegal drugs and drug activity; the use of alcohol; and the individual's mental health history.

28. Including instructions, the current online version of the SF-85P is 12 pages in length.

29. A completed, current version of the SF-86 (Form Approved OMB No. 3206 0005) can contain, inter alia, the following information about the individual who has completed it: Social Security number; passport information; citizenship; previous residence information; education; employment history; selective service record; military history; persons who know the individual well; marital status; relatives; foreign contacts; foreign activities; foreign business, professional activities, and government contacts; foreign travel; psychological and emotional health; police record; illegal use of drugs and drug activity; use of alcohol; government investigation and clearance record; financial record; use of information technology systems; involvement in non-criminal court actions; and association record.

30. The current version of the SF-86 includes an "Authorization for Release of Information" similar in content to authorization described in Paragraph 25 for the SF-85P.

31. The current version of the SF-86 includes an "Authorization for Release of Medical Information Pursuant to the Health Insurance Portability and Accountability Act (HIPAA)" similar in content to the authorization described in Paragraph 26 for the SF-85P.

32. Including instructions, the current online version of the SF-86 is 127 pages in length.

33. During her June 16, 2015 testimony before the House Committee on Oversight and Government Reform, then-Director of OPM, Katherine Archuleta,

confirmed that persons who had filed SF-86 had been affected by the breach by answering the following question from Rep. Chaffetz concerning the scope of the cyber intrusion:

> Q: Does it include anybody who's filled out SF-86, the standard form 86?
>
> A: The individuals who have completed an SF-86 and – may be included in that. We can provide any additional information in a classified setting.

OPM: Data Breach: Hearing Before the House Comm. On Oversight and Gov't Reform, 114th Cong. 14 (2015) (testimony of Katherine Archuleta, Director, Office of Personnel Management).

34. During her June 16, 2015 testimony before the House Committee on Oversight and Government Reform, Donna Seymour, then-OPM Chief Information Officer, confirmed that persons who had filed SF-86s had been affected by the breach by answering the following question from Rep. Cummings:

> Q: What can you tell us about the type of personal information that was compromised in this breach?
>
> A: The type of information involved in the personnel records breach [the "First Breach"] includes typical information about job assignment, some performance ratings, not evaluations, but performance ratings, as well as training records for our personnel. The information involved in the background investigations incident [the "Second Breach"] involves SF 86 data, as well as clearance adjudication information.

Id. at 16 (testimony of Donna Seymour, Chief Information Officer, Office of Personnel Management).

35. During her June 16, 2015 testimony, Ms. Seymour confirmed that information related to affected individuals' entire careers had been affected by answering the following questions from Rep. Cummings:

Q: Ms. Seymour, it was reported on Friday that in addition to this breach, hackers had breached highly sensitive information gathered in background investigations of current and former federal employees. Is that true?

A: Yes, sir, that is.

Q: Do you know how far back that goes?

A: No, sir, I don't. These are – the issue is that these are longitudinal records, so they span an employee's you know, career. And so I do not know what the oldest record is.

Q: So, it's possible that somebody could be working for the federal government for 30 years. And their information over that 30 years could've been breached?

A: Yes, sir. These records do span an employee's career.

Id.

OPM's Failure to Protect Plaintiffs' Personal Information

36. The Federal Information Security Management Act (FISMA), 44 U.S.C. § 3541 et. seq., makes the head of each agency, including the Defendant, responsible for providing information security protections and ensuring that agency officials take steps to reduce the risk of unauthorized use of information in the agency's possession.

37. FISMA further provides that each agency head, including the Defendant, is responsible for complying with the requirements of the statute and pertinent information technology policies, procedures, standards, and guidelines established by appropriate authorities, such as executive orders on cybersecurity and standards promulgated by the National Institute of Standards and Technology (NIST), 44 U.S.C. § 3554(a)(1)(B).

38. As the Inspector General reports and testimony discussed below demonstrate, Defendant failed to satisfy her responsibilities under FISMA and other applicable authority, a failure that is relevant because it is illustrative of Defendant's broader reckless disregard of Plaintiffs' informational privacy rights.

39. As recorded in a June 16, 2015 written statement submitted to the House Committee on Oversight and Government Reform, when Director Archuleta was sworn in 18 months earlier, she "immediately became aware of security vulnerabilities" in OPM's systems. OPM: Data Breach: Hearing Before the House Comm. On Oversight and Gov't Reform, 114th Cong. 6 (2015) (testimony of Katherine Archuleta, Director, Office of Personnel Management).

40. Director Archuleta repeated the assertions described in Paragraph 39 in a written statement submitted to the Senate Subcommittee on Financial Services and General Government. Federal IT Spending/OPM Data Security: Hearing Before the Subcommittee on Financial Servs. and General Gov't, Senate Comm. on Appropriations, 114th Cong. 4-5 (2015) (statement of Katherine Archuleta, Director, Office of Personnel Management).

41. In its audit report for Fiscal Year 2014, required by FISMA, OPM's Office of the Inspector General (OPM OIG) documented numerous deficiencies in OPM's information technology (IT) security program and practices. Office of Personnel Management, Office of Inspector General, Audit Report 4A-C1, 00-14-016 (Nov. 12, 2014).

42. In a June 16, 2015 written statement submitted to the House Committee on Oversight and Government Reform, OPM Assistant Inspector General for Audits, Michael R. Esser, described the audits of OPM's information technology security programs and practices that his office had performed under FISMA. OPM: Data Breach: Hearing Before the House Comm. on Oversight and Gov't Reform, 114th Cong. (2015) (statement of Michael Esser, Asst. Inspector General for Audits, Office of Personnel Management), available at www.democrats.oversight.house.gov/legislation/hearings/full-Committee-hearing-OPM-data-breach (hereinafter "Esser Statement").

43. In his June 16, 2015 written statement, Mr. Esser described some of the problems identified in these audits as dating back to Fiscal Year 2007. Id. Mr. Esser identified three of the "most significant issues identified in our FY 2014 FISMA audit" as being "Information Security Governance," "Security Assessment and Authorization," and "Technical Security and Controls." Id.

44. In his June 16, 2015 written statement, Mr. Esser described "Information Security Governance" as the "management structure and processes that form the foundation of a successful technology security program." Id. He described a "material weakness," defined as "a severe control deficiency that prohibits the organization from adequately protecting its data," in OPM's security governance practices. Id. First identified as a material weakness in the Fiscal Year 2007 report, his office "continued to identify this security governance issue as a material weakness in all subsequent FISMA audits through FY 2013." Id.

Although his office's Fiscal Year 2014 report classified this issue as a less serious "significant deficiency," he stated that OPM "continues to be negatively impacted by years of decentralized security governance" causing its technical infrastructure to remain "fragmented and therefore inherently difficult to protect." Id.

45. In his June 16, 2015 written statement, Mr. Esser described "Security Assessment and Authorization" as a "comprehensive assessment of each IT system to ensure that it meets the applicable security standards before allowing the system to operate in an agency's technical environment." Id. He stated that the "Office of Management and Budget (OMB) mandates that all Federal information systems have a valid Authorization." Id. After being removed as a concern in the FY 2012 audit report, problems recurred such that in FY 2014, "21 OPM systems were due for an Authorization, but 11 of those were not completed on time and were therefore operating without a valid Authorization." Id. Because they were operating without Authorization, his office recommended that these eleven systems be shut down, but none were shut down. Id.

46. In his June 16, 2015 written statement, Mr. Esser noted that two of the eleven OPM systems operating without an Authorization were general support systems on which "over 65 percent of all systems operated by OPM" reside. Id. at 4. Two others are owned by OPM's Federal Investigative Service, which, Mr. Esser, explained, "is responsible for facilitating background investigations for suitability and clearance determinations." Id. Mr. Esser's office believed that "the volume and sensitivity of OPM systems that are operating without an active Authorization

represents a material weakness in the internal control structure of the agency's IT security program." Id.

47. In his June 16, 2015 written statement addressing "Technical Security Controls," Mr. Esser referred to 29 audit recommendations in the Fiscal Year 2014 FISMA report and stated that "two of the most critical areas in which OPM needs to improve its technical security controls relate to configuration management and authentication of IT systems using personal identity verification (PIV) credentials." Id.

48. In his June 16, 2015 written statement, Mr. Esser described "configuration management" as referring to the "policies, procedures, and technical controls used to ensure that IT systems are securely deployed." Id. His office's Fiscal Year 2014 audit determined that some of OPM's regular system vulnerability scans "were not working correctly because the tools did not have the proper credentials, and that some servers were not scanned at all." Id. Another system security tool "was receiving data from only eighty percent of OPM's major IT systems." Id.

49. In his June 16, 2015 written statement, Mr. Esser noted that his office had determined that OPM "does not maintain an accurate centralized inventory of all servers and data bases that reside within the network. Even if the tools I just referenced were being used appropriately, OPM cannot fully defend its network without a comprehensive list of assets that need to be protected and monitored." Id. at 4-5. An agency is required to develop and maintain an inventory of its

information systems and audit all activities associated with those information system configurations. See NIST SP 800-53 Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations (Apr. 30, 2014).

50. In his June 16, 2015 written statement, Mr. Esser stated that, despite OMB requirements, "none of the agency's major applications require [personal identity verification] authentication. Full implementation of PIV verification would go a long way in protecting an agency from security breaches, as an attacker would need to compromise more than a username and password to gain unauthorized access to a system. Consequently, we believe that PIV authentication for all systems should be a top priority by OPM." Esser Statement at 5.

51. During her June 16, 2015 testimony before the House Committee on Oversight and Government Reform, Director Archuleta confirmed that Social Security numbers of individuals affected by the breaches were not encrypted by answering the following question from Rep. Lynch:

> Q: So were the Social Security numbers – were they Encrypted, yes or no?
>
> A: No, they were not encrypted.

OPM: Data Breach: Hearing Before the House Comm. On Oversight and Gov't Reform, 114th Cong. 14 (2015) (testimony of Katherine Archuleta, Director, Office of Personnel Management).

52. During her June 16, 2015 testimony, Director Archuleta confirmed that compromised data was not encrypted by answering the following questions from Rep. Walker:

> Q: Ms. Archuleta, it appears that OPM did not follow the very basic cybersecurity best practices, specifically such as network segmentation and encryption of sensitive data. Should the data have been encrypted? Can you address that?
>
> A: (OFF-MIKE) that the data was not encrypted. And as Dr. Ozment has indicated, encryption may not have been a valuable tool, and in this particular breach. As I said earlier, we are working closely to determine what sorts of additional tools we can put into our system to prevent further . . .
>
> (CROSSTALK)
>
> Q: To use your word you said may not have been. But that didn't answer the question should it have been encrypted? And could that have been another line of defense?
>
> A: I would turn to my colleagues from DHS to determine the use of encryption. But I will say that it was not encrypted at the time of the breach.

Id. at 28.

53. In a June 23, 2015 written statement submitted to the Senate Committee on Appropriations, Subcommittee on Financial Services and General Government, Mr. Esser again discussed his office's findings, including another discussion of the issues of "Information Security Governance," "Security Assessment and Authorization," and "Technical Security Controls." IT Spending and Data Security at OPM: Hearing Before the Subcommittee on Financial Servs. and General Gov't, Senate Comm. on Appropriations, 114th Cong. (2015) (statement of Michael Esser, Asst. Inspector General for Audits, Office of Personnel Management), available at www.appropriations.senate.gov.

54. In his June 23, 2015 written statement, Mr. Esser stated, "[a]lthough OPM has made progress in certain areas, some of the current problems and

weaknesses were identified as far back as Fiscal Year (FY) 2007. We believe this long history of systemic failures to properly manage its IT infrastructure may have ultimately led to the breaches we are discussing today." Id. at 1.

55. During his June 23, 2015 testimony before the Senate Committee on Appropriations, Subcommittee on Financial Services and General Government, Richard Spires, Former Chief Information Officer of the U.S. Department of Homeland Security and Internal Revenue Service, and current CEO of Resilient Network Systems, Inc. offered his expert opinion that OPM's deficient security practices could be expected to have resulted in the breaches when he answered the following question from Senator Moran:

> Q: . . . let me first start with a – with a broader question. Based on your understanding of the facts involved here and your best judgement, was the –was the breaches that have occurred at OPM, were they predictable based upon what we knew, looking at the – for example the OIG report. If you saw those reports, is this an outcome that could be expected.
>
> A: I think it is an outcome that could be expected, sir.

Id. at 15 (testimony of Richard Spires, Former Chief Information Officer, U.S. Department of Homeland Security and Internal Revenue Service).

56. During his June 24, 2015 testimony before the House Committee on Oversight and Government Reform, OPM Inspector General Patrick McFarland offered his expert opinion that OPM's deficient security practices exacerbated the possibility of the breaches when he answered the following question from Rep. Lynch:

> Q: OK. And the former chief technology officer at the IRS and the Department of Homeland Security said that the breaches were bound to happen given OPM's failure to update its cybersecurity. Is that – is that your assessment, Mr. McFarland?
>
> A: Well, I think without question it exacerbated the possibility, yes.

OPM Data Breach: Part II: Hearing Before the House Comm. on Oversight and Gov't Reform, 114th Cong. 30 (2015) (testimony of Patrick McFarland, Inspector General, Office of Personnel Management), available at www.cq.com.

57. In a recent media interview Clifton Triplett, OPM's senior cybersecurity advisor, reflecting back on the breaches and the "emergency IT security upgrades" required in their wake, conceded, "[w]e're a wonder poster child of how bad it can be if you don't do the right thing." Jack Moore, OPM: A Year After the Big Breach, Nextgov.com (May 11, 2016), available at, www.nextgov.com/cybersecurity/2016/05/opm-year-after-big-breach/128233.

58. By the conduct described in Paragraphs 36-57, the Defendant has shown a reckless indifference to her obligation to protect the personal information of current and former federal employees, including NTEU's members—such as Plaintiffs Gambardella, Howell, and Ortino—from unauthorized disclosure.

NTEU Members Have Been Injured by Defendant's Failure to Protect Their Personal Information

59. An unknown number of NTEU members, including Plaintiffs Gambardella, Howell, and Ortino, have been identified by OPM as having been affected by the breaches described in Paragraphs 13-19 and have been sent the notifications described in Paragraphs 13 and 15.

60. An unknown number of NTEU members, including Plaintiffs Gambardella, Howell, and Ortino, submitted, as part of a background investigation, current or previous versions of SF-86 that resided in an OPM data system at the time of the unauthorized data access and taking announced by OPM on June 12, 2015.

61. Personal information gathered by investigators (from interviews and other sources) as part of investigations of NTEU members who submitted a SF-86, including Plaintiffs Gambardella, Howell, and Ortino, resided in an OPM data system at the time of the breach announced by OPM on June 12, 2015.

62. The personal information described in Paragraphs 60 and 61 has been subject to unauthorized access and taking by those who perpetrated the breach announced on June 12, 2015.

63. An unknown number of NTEU members, including Plaintiff Gambardella, submitted, as part of a background investigation, current or previous versions of SF-85 or SF-85P that resided in an OPM data system at the time of the unauthorized data access and taking announced by OPM on June 12, 2015.

64. Personal information gathered by investigators (from interviews and other sources) as part of the investigation of NTEU members, including Plaintiff Gambardella, who submitted SF-85 and SF-85P resided in an OPM data system at the time of the breach announced on June 12, 2015.

65. Upon information and belief, the personal information described in Paragraphs 63 and 64 was subject to unauthorized access and taking by those who perpetrated the breach announced on June 12, 2015.

66. NTEU members, including Plaintiffs Gambardella, Howell, and Ortino, submitted the types of inherently personal information described in Paragraphs 21-32 to OPM and that information resided on the breached OPM databases. NTEU members, including Plaintiffs Gambardella, Howell, and Ortino submitted that inherently personal information with reason to believe, based on assurances from the government, that the information would be safeguarded from unauthorized disclosure.

67. The current version of the SF-85 contains the following statement on the second page:

> Disclosure of Information
>
> The information you give us is for the purpose of determining your suitability for Federal employment; we will protect it from unauthorized disclosure. The collection, maintenance, and disclosure of background investigative information is governed by the Privacy Act.

68. The current version of the SF-85P contains the following statement on the second page:

> Disclosure of Information
>
> The information you give us is for the purpose of investigating you for a position; we will protect it from unauthorized disclosure. The collection, maintenance and disclosure of background investigative information is governed by the Privacy Act.

69. The current version of the SF-86 contains the following statement on the second page:

> Disclosure of Information
>
> The information you provide is for the purpose of investigating you for a national security position, and the information will be protected from unauthorized disclosure. The collection, maintenance, and disclosure of background investigative information are governed by the Privacy Act.

70. Upon information and belief, previous versions of the SF-85, SF-85P, and SF-86 contained statements similar in content to those set forth in Paragraphs 67-69.

71. Plaintiffs Gambardella, Howell, and Ortino were notified by OPM that they were affected by the data breach announced on June 4, 2015.

72. Plaintiffs Gambardella and Howell were notified by OPM that they were affected by the data breach announced on June 12, 2015. Each has inherently personal information that resided and continues to reside on OPM's information systems as part of his or her background investigation(s) related to federal employment.

73. NTEU represents thousands of other members who have been notified by OPM that they were affected by the data breach announced on June 4, 2015.

74. NTEU likewise represents thousands of other members who have personal information stored on OPM's information systems and who have been notified by OPM that they were affected by the data breach announced on June 12,

2015, and who have, as part of background investigations related to federal employment, submitted an SF-85, SF-85P, or SF-86 to OPM.

75. The Defendant showed reckless indifference to her obligation to protect personal information provided by NTEU members—including Plaintiffs Gambardella, Howell, and Ortino—with the assurance that the information would be safeguarded.

76. The harm to NTEU members, including Plaintiffs Gambardella, Howell, and Ortino occurred the moment that their inherently personal information—which they provided to OPM on the promise of confidentiality and as a condition of their federal employment—was taken by unauthorized intruders from OPM's databases. This constitutionally protected private information should have been properly protected from unauthorized access and taking by OPM, but was not, as described above.

77. The Defendant's reckless indifference to her obligations has deprived NTEU members, including Plaintiffs Gambardella, Howell, and Ortino, of the security that comes from knowing that the inherently personal information that they provided to the Defendant on the promise of confidentiality will be safeguarded and will not fall into the hands of third parties lacking authorization to view the information.

78. The Defendant's reckless indifference to her obligations has caused NTEU members, including Plaintiffs Gambardella, Howell, and Ortino, to lose that sense of security, which can only be restored through relief from this Court.

79. In or around February 2016, Plaintiff Gambardella attempted to electronically file a joint federal tax return for tax year 2015. He was unable to do so because, as the IRS notified him, an individual federal tax return had already been filed in his name for 2015. That individual federal tax return was fraudulently filed in Mr. Gambardella's name.

80. After learning of the fraudulently-filed return, Mr. Gambardella expended time and resources interfacing with IRS to deal with the issue of the already-filed fraudulent return. He then had to re-file his 2015 federal return. Due to the prior fraudulent filing, however, Mr. Gambardella could not file electronically, but had to file in paper form. He was unable to file until the end of February 2016. The paper federal return, which takes longer to process than an electronically filed return, was not processed by IRS until April 6, 2016.

81. Mr. Gambardella believes he is entitled to a federal tax refund of approximately $7,000. However, as of the filing of this amended complaint, Mr. Gambardella still has not received his federal tax refund.

82. Apart from the OPM data breaches announced in June 2015, Mr. Gambardella has not, to the best of his knowledge, had his personal information exposed in any other public or private sector data breach. Nor has he, to the best of his knowledge, ever been the victim of identity theft other than the instances described in this amended complaint.

83. Because the data breaches announced in June 2015 are the only data breaches that have implicated his personal information, Mr. Gambardella

reasonably believes that the fraudulent federal tax return, which has led to a delay in his approximately $7000 federal tax refund, stems from the OPM data breaches. This delay has led to a loss of use of the refund money and a loss of interest on that money.

84. Mr. Gambardella has experienced other harm that he reasonably believes, given that he has not been affected by any other breaches, is attributable to the breaches announced in June 2015. Earlier this year, he had three separate fraudulent charges appear on an existing credit card. Each was for an amount over $300. He was able to have those fraudulent charges resolved after contacting his credit card company.

85. Apart from the OPM data breaches announced in June 2015, Plaintiff Howell has not had, to the best of his knowledge, his personal information exposed in any other public or private sector data breach.

86. Apart from the OPM data breaches announced in June 2015, Plaintiff Ortino has not had, to the best of his knowledge, his personal information exposed in any other public or private sector data breach.

87. Plaintiffs Gambardella, Howell, and Ortino, and other NTEU members who were notified that they were implicated by one or both of the breaches announced in June 2015, have reason to believe that, given the June 2015 breaches and OPM's continued inadequate security measures, the personal information that they have entrusted to the Defendant on the promise of confidentiality is at substantial risk of further unauthorized access. They reasonably believe that the

risk will not be abated until OPM is ordered to correct the security deficiencies discussed above. Each unauthorized access to the personal information that they have entrusted to OPM further violates their constitutional right to informational privacy.

88. The substantial risk of another unauthorized access of this personal information is further evidenced by OPM OIG's Final Audit Report for Fiscal Year 2015, issued on November 10, 2015. In that report, the OIG explained that "for many years, we have reported critical weaknesses in OPM's ability to manage its IT environment, and warned that he agency was at an increased risk of a data breach." Report at 5. Yet, "OPM continuously failed a variety of FISMA metrics and carried material weaknesses in the annual FISMA reports." Id. Indeed, the OIG concluded, "[o]ur recommendations appeared to garner little attention, as the same findings were repeated year after year." Id. The OIG added that in light of "the overall lack of compliance that seems to permeate the agency's IT security program," "we are very concerned that the agency's systems will not be protected against another attack." Id.

89. In the same fiscal year 2015 audit report, the OIG noted that of particular concern was OPM's continued "inability to accurately inventory its systems and network devices," which "drastically diminishes the effectiveness of its security controls." Id. at 6. While, in the wake of the data breaches announced in June 2015, "OPM has implemented a large number of improved security monitoring tools," "without a complete understanding of its network, it cannot adequately

monitor its environment and therefore the usefulness of these tools is reduced." Id. "This same concern extends to OPM's vulnerability scanning program." Id.

90. Further demonstrating the substantial risk of another unauthorized access of the personal information of Plaintiffs Gambardella, Howell, and Ortino and other NTEU members is OPM's flawed effort to secure an able contractor to overhaul its information technology security. In July 2015, OPM awarded a sole source control award to Imperatis, formerly known as Jorge Scientific Corporation, to overhaul OPM's IT infrastructure. Senator Claire McCaskill wrote to then-Director Archuleta expressing concern about its decision to "rush the award, and its decision to not engage in a full and open competition." See Letter from Hon. Claire McCaskill to Hon. Beth Cobert dated May 13, 2016 (reiterating previously aired concerns). She was particularly concerned about the "history of misbehavior of the company's employees." Id. In light of the company's "troubled history with government contracting," Senator McCaskill was "not entirely surprised" when her office was informed on May 10 that Imperatis "had abruptly ceased operations" on its contract with OPM. Id. Indeed, on May 9, Imperatis "stopped coming to work," causing OPM to terminate the company's contract that same day," even though Imperatis "had about a month of work left under the deal." Jason Miller, Vendor Hired to Improve Security of OPM's Network Goes Out of Business, federalnewsradio.com (May 16, 2016) (noting that "Imperatis referenced financial distress at the company as the reason for the immediate closure"). The status of

Imperatis's now abandoned effort to overhaul OPM's information technology infrastructure is unknown.

91. OPM's OIG continues to express concern over OPM's plan to upgrade its information technology security, further highlighting the substantial risk of another unauthorized access of the personal information of Plaintiffs Gambardella, Howell, and Ortino and other NTEU members. OPM's OIG, in an interim status report issued on May 18, 2016, expressed continued concern about OPM's efforts to upgrade its information technology security and, in particular, its failure to properly develop a proper project plan for the upgrade in accordance with OMB requirements. As OPM's OIG noted, nearly a year ago, it "expressed the opinion that OPM's desire to better secure its IT environment as quickly as possible, [which led to its] declining to perform many of the mandatory planning steps [required for such a project by OMB], resulted in a high risk that the Project would fail to meet its objectives." Report at 3. That risk, OPM's OIG reports, has only grown. As it stated, "[n]ow that we have reviewed OPM's recent Business Case and its support activities in depth, we are even more concerned about the lack of disciplined capital planning processes." Id. at 3-4 (noting that "OPM did not develop a realistic budget based on an understanding of the number of systems that would need to be migrated to the new [information technology] environment, the level of effort associated with the required modernization and security updates, and the cost of this process").

92. The Defendant's reckless indifference to her obligations has put NTEU members, including Plaintiffs Gambardella, Howell, and Ortino, and their families, friends, and other associates at substantial risk of identity theft, thereby subjecting them to financial peril and inconvenience.

93. The Defendant's reckless indifference to her obligations has put NTEU members, Plaintiffs Gambardella, Howell, and Ortino, and their families, friends, and other associates at substantial risk of harassment, intimidation, or coercion.

94. The Defendant's reckless indifference to her obligations has caused NTEU members, including Plaintiffs Gambardella, Howell, and Ortino, emotional distress and anxiety over the effect that these data breaches will have on them, their families, friends, and other associates.

CAUSE OF ACTION

95. Plaintiffs reassert the allegations contained in paragraphs 1 through 94 of this complaint as though contained herein.

96. The Defendant has a duty to safeguard NTEU members' personal information. NTEU members, including Plaintiffs Gambardella, Howell, and Ortino, submitted much of the information at issue in this complaint during background investigations required for appointment to, or retention in, their federal positions. To get, or keep, their jobs, NTEU members, including Plaintiffs Gambardella, Howell, and Ortino, had no choice but to divulge information which they would otherwise prefer be kept confidential. This sensitive information was

disclosed to the federal employer, and stored in the Defendant's data systems, with the express assurance that it would be protected from unauthorized disclosure.

97. By failing to heed the repeated warnings of OPM's OIG and otherwise failing to satisfy obligations imposed on her by statute and other appropriate authority, the Defendant has manifested reckless indifference to her obligation to safeguard personal information provided by NTEU members, including Plaintiffs Gambardella, Howell, and Ortino, with the assurance that it would be protected against unauthorized disclosure.

98. The Defendant has violated Plaintiffs Gambardella, Howell, and Ortino's constitutional right to informational privacy, including their right to due process under the Fifth Amendment to the U.S. Constitution. The Defendant has likewise violated the constitutional right of informational privacy of all other NTEU members whose personal information was exposed by the breaches announced on June 4, 2015 and June 12, 2015.

REQUEST FOR RELIEF

WHEREFORE, based on the foregoing, the Plaintiffs request judgment against the Defendant:

A. Declaring that the Defendant's failure to protect NTEU members' personal information was unconstitutional;

B. Ordering the Defendant to provide lifetime credit monitoring and identity theft protection to NTEU members, at no cost to those NTEU members;

C. Ordering the Defendant to take immediately all necessary and appropriate steps to correct deficiencies in OPM's IT security program so that NTEU members' personal information will be protected from unauthorized disclosure;

D. Enjoining the Defendant from collecting or requiring the submission of NTEU members' personal information in an electronic form or storing any such information in an electronic form until the Court is satisfied that all necessary and appropriate steps to safeguard NTEU members' personal information have been implemented;

E. Awarding Plaintiffs their reasonable attorney fees and costs incurred;

F. Ordering such further relief as the Court may deem just and appropriate.

Respectfully submitted,

Gregory O'Duden
Larry J. Adkins

/s/ Paras N. Shah

Paras N. Shah
Allison C. Giles
NATIONAL TREASURY EMPLOYEES UNION
1750 H Street, N.W.
Washington, D.C. 20006
Tel: (202) 572-5500
Fax: (202) 572-5645
Email: greg.oduden@nteu.org
Email: larry.adkins@nteu.org
Email: paras.shah@nteu.org
Email: allie.giles@nteu.org

Attorneys for Plaintiffs

Of Counsel:

Leon O. Dayan
Devki K. Virk
BREDHOFF & KAISER PLLC
805 15th Street N.W.
Suite 1000
Washington, D.C. 20005
Tel: (202) 842-2600
Fax: (202) 842-1888
Email: ldayan@bredhoff.com
Email: dvirk@bredhoff.com

Attorneys for Plaintiffs

June 3, 2016

CERTIFICATE OF SERVICE

I hereby certify that on June 3, 2016, I filed the above amended complaint with the Court's CM/ECF system, which will send notice to the other parties.

/s/ Paras N. Shah
Paras N. Shah

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN RE U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY LITIGATION This Document Relates To: *NTEU v. Cobert*, 15-cv-1808-ABJ (D.D.C.) 3:15-cv-03144 (N.D. Cal.)	Misc. Action No. 15-1394 MDL Docket No. 2664

NOTICE

Plaintiffs National Treasury Employees Union (NTEU), Eugene Gambardella, Stephen Howell, and Jonathon Ortino (collectively, NTEU Plaintiffs) respectfully provide this update on the status of Plaintiff Gambardella's delayed federal tax refund, which has now been received. In their amended complaint, NTEU Plaintiffs alleged that, in the aftermath the Office of Personnel Management data breaches, Mr. Gambardella was the victim of a fraudulent federal tax return. Am. Compl. ¶ 79. That fraudulent return delayed his ability to properly file his federal tax return; when he was able to file it in February 2016, he had to do so in paper form, causing more delays. Id. ¶ 80. As of the filing of the June 3 amended complaint, Mr. Gambardella had yet to receive his expected refund of approximately $7,000. Id. ¶¶ 80-81. Thus, NTEU Plaintiffs alleged that the delay had "led to a loss of use of the refund money and a loss of interest on that money." Id. ¶ 83.

Mr. Gambardella recently received his full federal tax refund, with interest. NTEU Plaintiffs bring this development to the Court's attention for the sake of completeness; they do not believe that it adversely affects their Article III standing.

Respectfully submitted,

Gregory O'Duden
Larry J. Adkins

/s/Paras N. Shah
Paras N. Shah
Allison C. Giles
NATIONAL TREASURY EMPLOYEES UNION
1750 H Street, N.W.
Washington, D.C. 20006
Tel: (202) 572-5500
Email: greg.oduden@nteu.org
Email: larry.adkins@nteu.org
Email: paras.shah@nteu.org
Email: allie.giles@nteu.org

Counsel for NTEU Plaintiffs

Of Counsel:

Leon O. Dayan
Devki K. Virk
BREDHOFF & KAISER PLLC
805 15th Street N.W.
Suite 1000
Washington, D.C. 20005
Tel: (202) 842-2600
Email: ldayan@bredhoff.com
Email: dvirk@bredhoff.com

October 13, 2016

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

In re: U.S. Office of Personnel Management Data Security Breach Litigation,	) Civil Action No. 15-mc-1394) MOTIONS HEARING) Washington, DC) October 27, 2016) Time: 10:00 A.M.

TRANSCRIPT OF MOTIONS HEARING
HELD BEFORE
THE HONORABLE JUDGE AMY BERMAN JACKSON
UNITED STATES DISTRICT JUDGE

A P P E A R A N C E S

For the Plaintiffs:

Daniel Girard, Esq.
Jordan Elias, Esq.
Girard, Gibbs
601 California Street
14th Floor
San Francisco, CA 94108

Peter A. Patterson, Esq.
Cooper & Kirk
1523 New Hampshire Avenue N.W.
Washington, DC 20036

Paras Shah, Esq.
Bredhoff & Kaiser
805 Fifteenth Street N.W.
Washington, DC 20005

Government Counsel:

Matthew A. Josephson, Esq.
U.S. Department of Justice
Civil Division
20 Massachusetts Avenue N.W.
Washington, DC 20530

KeyPoint Counsel: **F. Joseph Warin, Esq.**
Jason J. Mendro, Esq.
Gibson, Dunn & Crutcher
1050 Connecticut Avenue N.W.
Washington, DC 20036

Court Reporter: Janice E. Dickman, RMR, CRR
Official Court Reporter
United States Courthouse, Room 6523
333 Constitution Avenue, NW
Washington, DC 20001
202-354-3267

* * * * * * * PROCEEDINGS * * * * * * *

THE COURTROOM DEPUTY: Your Honor, calling case number 15-MC-1394. In re: U.S. Office of Personnel Management Data Security Breach Litigation.

Will counsel for the -- arguing counsel for the parties please come to the lectern, identify yourself for the record and the party or parties that you represent.

MR. GIRARD: Good morning, Your Honor. Dan Girard for the class plaintiffs.

THE COURT: Good morning.

MR. ELIAS: Good morning. I'm Jordan Elias for the plaintiffs.

THE COURT: Good morning.

MR. PATTERSON: Good morning, Pete Patterson for the plaintiffs.

THE COURT: Morning. You're all arguing? Different issues?

MR. GIRARD: Yes.

THE COURT: Okay.

MR. SHAH: Good morning, Your Honor. Paras Shah, counsel for NTEU plaintiffs.

THE COURT: Good morning.

MR. JOSEPHSON: Good morning, Your Honor. Matt Josephson, Office of Personnel Management.

MR. WARIN: Good morning, Your Honor. Joseph

Warin from Gibson, Dunn and Crutcher representing KeyPoint.

THE COURT: Good morning.

MR. MENDRO: Good morning, Your Honor. Jason Mendro for KeyPoint Government Solutions.

THE COURT: Okay. All right. Good morning, everyone. It's been a long time since you've all been here, but you've done a lot of work and I want to say right off the bat that I really appreciated the quality of the briefs and the fact that they lacked any of the sarcasm and tone that a lot of the briefs I often receive contain. They were very professional and civil and thorough and I appreciated that.

We're here today for the first hearing on defendants' motions to dismiss the consolidated amended complaint and the multidistrict litigation arising out of the OPM data breach, and the complaint filed by the National Treasury Employees Union, which has now been consolidated with all the other complaints.

Plaintiffs have brought claims under the Privacy Act, the Little Tucker Act and the APA against OPM and claims under the Fair Credit Reporting Act, as well as state statutes and state common law principles against KeyPoint Government Solutions, which is the government contractor. NTEU has also brought a constitutional claim.

Defendants have moved to dismiss the complaints on

multiple grounds, including on the ground that the Court lacks subject matter jurisdiction to hear it because the plaintiffs don't have standing to bring the lawsuit.

Given the complexity of the standing issue and the fact that the Court must, as a matter of constitutional principle, determine the question of standing before going on to consider the arguments addressed to the claims on the merits. Indeed, because in the absence of standing I don't even have the power to consider the claims on the merits.

I informed everyone that today we would only hear arguments on some of the issues raised in the motions to dismiss: Whether plaintiffs have standing under Article III of the U.S. Constitution to bring these claims against OPM and KeyPoint; whether, even if they have standing, plaintiffs have alleged that they've suffered the monetary loss necessary to bring an action for damages under the Privacy Act, and; whether the claims against KeyPoint are barred by government contractor immunity.

I want to underscore that no one should view the fact that I bifurcated the hearing as a sign that I've already decided the issue and don't plan to consider the merits. While the quality of the briefing has been excellent on every issue and I have more than enough from the parties to decide all these issues based on the briefs alone, I do want to ask some questions about the standing

and hear what everyone has to say. But I do intend to utilize the second hearing date we've already put on the calendar to give you the opportunity to address some of the other issues in the event I need to or decide to address them in my opinion.

So that's set for November 10 at 10 a.m. I would like to make it 9:30, unless that poses a difficulty for the counsel who will be arguing.

So I'm going to hear from both sides on the standing and damages issue, which I think really are very closely related, and then go on to the contractor immunity issue.

Also, I want to encourage everyone not to draw any conclusions about how I'm thinking from the fact that pointed questions may be posed to one side or the other. If any of you have ever been to any of my other hearings, you know that that's just an occupational hazard of walking into this courtroom.

There's no disagreement here about what the legal requirement is or that it is essential to establish all the elements of constitutional standing before the Court has the power to consider the merits. The Supreme Court, in the *Lujan* case, set out the standard and it hasn't been changed in any of the other cases that everyone cites. It's the plaintiffs' burden to demonstrate that they have standing,

which is the first element of the justiciable case or controversy under Article III, and standing consists of multiple things.

First of all, an injury in fact, which itself has two components, it has to be harm that is concrete and particularized, and the Supreme Court said in *Spokeo* that means both concrete and particularized, and harm that is actual or imminent and not merely conjectural or hypothetical.

So you have to establish all of those pieces to get to the first element of standing, which is injury in fact. And then in addition to the injury in fact, plaintiff must also plead facts that would establish that the injury is fairly traceable to the challenged action of the defendant, which is the causation requirement, and that it's likely, as opposed to merely speculative, that it could be redressed by a favorable decision in the case.

So that's the legal backdrop for the motions before me today. I'm going to want to hear from both sides about both injury in fact and causation. And since it's the government's motion, I'll let you start.

MR. JOSEPHSON: Good morning, Your Honor. Matt Josephson on behalf of the Office of Personnel Management.

This case should be dismissed for two reasons. First, plaintiffs have failed to establish Article III standing. Plaintiffs have not pled facts plausibly showing

that they have sustained a concrete, actual, and imminent injury that is fairly traceable to the OPM cybersecurity incidents.

Second, even if a particular plaintiff could establish Article III standing, that plaintiff's claims under the Privacy Act should be dismissed for failure to specially plead actual damages.

With respect to Article III standing, plaintiffs allege both past harms and future harms in the consolidated amended complaint. I would like to start with the allegations of past harms and then move to allegations of future harms, unless the Court has specific questions about a particular category.

THE COURT: Well, let me just start by asking, does the motion to dismiss on standing grounds cover all the counts, including the contract claim on behalf of the questionnaire class? Or is that count simply subject to the 12(b)(6) motion?

MR. JOSEPHSON: No, Your Honor, it would apply to all counts.

THE COURT: Okay. All right. I'll let you start before I start.

MR. JOSEPHSON: Regarding the allegations of past information misuse, there's one general deficiency that permeates all categories of injury, and that's causation.

The problem with the consolidated amended complaint is that the plaintiffs have not plausibly pled facts that would connect a particular category of injury to a particular type of information at issue in this particular incident. Instead, the plaintiffs have pled, in scattershot fashion, a variety of injuries that bear no relation to each other, nor to this particular data breach.

The first category of past information misuse that plaintiffs allege is financial fraud. There are 15 plaintiffs who alleged that financial fraud has occurred in their existing accounts or in a new account that's been opened in their name.

Regarding the existing accounts, the fundamental causal deficiency is that the plaintiffs do not allege, no plaintiff alleges that the account number that was used fraudulently was ever provided to OPM in the SF-86 as a part of the background investigation process. Not one plaintiff. That allegation is not in the consolidated amended complaint.

THE COURT: All right. And to tell you the truth, I don't really have a lot of questions about your causation argument about the financial irregularities, but I think there's a lot I want to talk about on the injury in fact aspect of some of the other claims. So I want to start there.

A lot of the standing cases that you cite, for instance, the D.C. Circuit opinion in the case involving the

Arizona sheriff, emphasize that a plaintiff can't pursue a generalized grievance to test the legality of government action in the abstract based on its alleged harm to the citizenry as a whole. But you're not alleging that that's what's really going on here, are you?

MR. JOSEPHSON: Well, our argument is that the plaintiffs -- it's the plaintiffs' burden to personally show standing. Each and every plaintiff has the burden that they specifically have been harmed in a concrete and particular way by this particular incident.

THE COURT: Right. But usually concreteness is to separate a case from one of these generalized abstract harm cases. And congress here, do you agree, that in the Privacy Act they created a duty owed to these plaintiffs personally to protect the security of their information?

MR. JOSEPHSON: That is correct. Congress created a cause of action, a limited cause of action under the Privacy Act which waived sovereign immunity for very specific and particular types of harm, namely, actual damages. And if there are not allegations that specially show actual damages, then the plaintiff has failed to state a claim under that particular statute.

THE COURT: Well, that's a failure to state a claim. So that assumes that there's standing. So do you -- are you saying that this case presents the sort of abstract

generalized concern that can't be an injury in fact, or are you saying that even -- maybe it is an injury in fact, but they haven't met the requirements of the Privacy Act?

MR. JOSEPHSON: We challenge both standing and actual damages in our motion to dismiss. In terms of the cases that discuss generalized grievances, oftentimes those cases concern claims that challenge -- generally challenge government policies.

THE COURT: I don't think this is that, do you?

MR. JOSEPHSON: Agreed. They're not challenging a statute or anything of that nature. However, it's still plaintiffs' burden to meet the requirements of Article III. As Your Honor laid out in the opening, those three requirements are well established and they have to plausibly plead facts for each and every one of those elements. And all 38 people in this particular case bear that burden. It's not sufficient for one plaintiff to point to another plaintiff and piggyback on those allegations.

THE COURT: Well, there was some hope that as the *Spokeo* case bubbled up through the circuit, that the Supreme Court would actually clarify what concrete and particularized means in the context of the statutory violation. And Justice Alito plainly reiterated that there has to be a concrete harm. He said Article III standing requires a concrete injury, even in the context of a statutory

violation. But then he said that doesn't mean that a risk of harm, material harm can't satisfy the requirement of concreteness. And he said a procedural violation in the statute can be sufficient in some circumstances and plaintiffs don't need to allege additional harm.

But then he also said not all violations cause harm or present a risk of harm. And then he didn't help us by defining what those circumstances would be. He remanded the case to the lower court to determine whether the particular violations alleged entail a degree of risk sufficient to meet the concreteness requirement.

So it seems to me that's what I have to decide, at least with respect to the people who are claiming a risk of harm, as opposed to the actual -- the financial issues. So where does this case fall on that spectrum?

MR. JOSEPHSON: Your Honor, I completely agree that that is the issue for the increased-risk plaintiffs. The Supreme Court has made very clear that for future injuries to meet the injury in fact standard, they must be certainly impending or there must be a substantial risk that that harm will in fact occur. And the D.C. Circuit has elaborated on that standard both in the *Public Citizen* case and the *Food & Water Watch* case that we cite in our papers, making clear that there has to be both a substantial risk of harm and a substantial probability that it will actually

happen.

Here -- well, and throughout the federal courts those principles have been applied in data breach cases and most Courts have come to the conclusion that future identity theft, the possibility that at some point a third-party criminal will use that information to the detriment of a particular plaintiff in a particular way is simply too speculative. There's too many links in that causal chain to conclude that it's an imminent harm. And that's our argument with respect to the increased-risk-of-harm plaintiffs.

THE COURT: So the issue is not that it's not concrete and particularized, it's that you don't have the second half; you don't have the imminence?

MR. JOSEPHSON: I think there's analytical overlap between the two.

THE COURT: Well, especially when he talked about a material risk of harm being a concrete harm, it seems like he was incorporating the second half into the first half.

MR. JOSEPHSON: We agree with that, Your Honor, yes.

THE COURT: Well, is it fair to say, though, that congress passed the Privacy Act because the disclosure of private information could pose a material risk of harm?

MR. JOSEPHSON: Yes, congress passed the Privacy Act to provide rules for federal agencies to follow in securing information. And they did create a limited cause

of action for damages, if very specific circumstances are present. And one of those circumstances is monetary loss. And as we have argued, that simply has not been shown by any of the 38 plaintiffs in this case.

THE COURT: Well, I've read the supplemental authorities the parties have pointed me to. Is there anything in this circuit post-*Spokeo* that's helpful? In the *Hancock* case the problem was that the plaintiffs alleged that the violation of the statute alone was injury in fact. But, it went on and distinguished that from a situation where the plaintiffs alleged an increased risk of identity theft or emotional injury. Is that telling me that the D.C. Circuit thinks that those are enough?

MR. JOSEPHSON: No, Your Honor. And the issue was never decided in *Hancock*. We simply agreed to the notice because it is an Article III -- it is a recent Article III standing case from the circuit that we wanted to bring to the Court's attention.

But I would like to highlight a couple points on the increased risk issue. The plaintiffs have emphasized in their papers that this was a targeted risk -- a targeted breach, that this was a data breach perpetuated in a sophisticated and malicious manner as alleged and that the individual responsible -- individuals responsible did so for purposes of obtaining the data. And they relied on that

fact in an effort to distinguish the data breach cases that don't involve targeted thefts at all. Those cases either involve lost data, or maybe stolen data, maybe a computer stolen, a thumb drive, something of that nature, but there's no indicia of intent to misuse.

I would point the Court towards Judge Cooper's recent decision in the *Attias, CareFirst* case where he addresses that very issue. And he explains that while the targeted nature of the theft does make the causal connection a little shorter, it does remove that speculative link in the chain. It's still speculative to conclude that even in a targeted breach, that a particular plaintiff will sustain a particular injury as a result of a particular type of future misuse. There's still a lot of speculation that has to eventualize in order for that injury to occur.

THE COURT: Well, you're getting right at something that I wanted to ask you about. It is interesting, one thing that is not mentioned in a single pleading in this case, and what is your point of view on the question of whether it's a matter of public record that this was a state sponsored cyber attack?

MR. JOSEPHSON: Well, Your Honor, for purposes of this motion we take the allegations in the complaint, the well-pled allegations in the complaint as true, and we test their legal sufficiency under the Federal Rules of Civil

Procedure. We think that that's the legal issue before the case [sic].

THE COURT: Well, but for subject matter jurisdiction, I'm allowed to go beyond the face of the complaint, aren't I?

MR. JOSEPHSON: That is true. The Court can consider extra pleading material for purposes of 12(b)(1) analysis.

THE COURT: Well, the congressional report -- they talk about the congressional investigation in the original complaint. The *Congressional Report*, on the first page, quotes former CIA director Michael Hayden as saying there is a treasure trove of information now available to the Chinese. *Forbes* magazine quotes intelligence officials and congressional officials as pointing to China. *The New York Times*, in July, said the Obama administration has determined that it must retaliate against China. And *The Washington Post*, in December, said the Chinese government has arrested the hackers that it says were connected to the breach.

Is this something that I should consider when we talk about the imminence of the harm? Because all the targeted thefts that they talk about are people who were targeting credit information and there was a reason to believe it's because that's what they wanted. Here, everything outside this room seems to suggest that what they wanted was intelligence information, which makes the

plaintiffs' claims significantly more attenuated. So am I supposed to think about that or am I not supposed to think about that?

MR. JOSEPHSON: Regarding that specific *Congressional Report*, we would take issue with whether that can be considered, whether -- whether reports like that are subject to judicial notice under the Federal Rules of Evidence. There's a good bit of case law that says they're not of the sufficient reliability to use in terms of facts, assuming that those facts are true. And we obviously take issue with a lot of the findings that the committee -- OPM takes issue with a lot of the findings that the committee made in that report.

The second point I would make, the report doesn't pertain to actual damages at all. It's completely irrelevant to the issue of whether a specific plaintiff has sustained a specific monetary loss.

THE COURT: Doesn't mention monetary losses. It talks about intelligence.

All right. So the government does not, I think it's plain, want me to pay any attention to any discussion whatsoever, even if it's in the public sphere, about who was behind this breach and what the purpose of the breach was?

MR. JOSEPHSON: For purposes of this motion, that's correct. I think we need to look at the allegations

in the complaint and determine whether they're sufficient to establish jurisdiction or a claim under the federal statutes that the plaintiffs have identified.

THE COURT: All right. Well, moving from concrete and particular to actual and imminent, does the fact that the government itself immediately offered free credit and identity theft monitoring services to the victims reflect the fact that the future harm is not merely conjectural or hypothetical?

MR. JOSEPHSON: No, Your Honor, it does not. And I would point the Court to Judge Boasberg's opinion in *SAIC* where he addresses this very issue. The question -- the standing question is whether there's a certainly impending harm for a particular plaintiff. It may be that the expense of credit monitoring services is a reasonable expense. Many defendants in data breach cases, not just OPM, but many large-scale retailers often provide credit monitoring services in the wake of a data breach.

THE COURT: But didn't the Court in *Neiman Marcus* actually find that that offer showed that the risk was not merely ephemeral?

MR. JOSEPHSON: Yes, there was a section in *Neiman Marcus* where the Seventh Circuit concluded that that particular portion of the opinion is, frankly, at odds with the certainly impending standards that the Supreme Court has

set in *Clapper* and other cases for future injury.

The provision of credit monitoring services can be a reasonable expense. OPM offered those very services in the wake of the incident. But it's a different issue to say that a particular individual in this case will imminently be harmed unless the Court provides a certain form of relief. That's a different level of analysis, it's more particularized, it's more stringent in terms of the imminency of the harm. It's just not -- it's not the same question to say the expense is reasonable and so, therefore, every plaintiff should be able to sue the government for it.

THE COURT: All right. Well, going back to the financial irregularities, I understand why you say that the allegations that there were unauthorized charges on debit or credit cards or fraudulent tax returns or other misuse of Social Security numbers isn't sufficient to allege actual monetary harm for Privacy Act purposes, but are those things alone enough to be actual injuries for standing purposes?

In other words, I know you say the cause -- also that the causation is insufficient, but are they injuries in fact and the only problem is there's no causation?

MR. JOSEPHSON: As we note in our reply, we have not challenged the fraudulent tax returns allegations and the allegations of Social Security number misuse on injury in fact grounds. We do very much challenge those

allegations on causation and think that there's been a complete absence of facts connecting those incidents, alleged incidents to this particular cybersecurity incident. But we have not challenged those two categories on injury in fact grounds. We have challenged the financial fraud categories --

THE COURT: You say they have to be unreimbursed not only for purposes of the Privacy Act, but also for purposes of injury in fact?

MR. JOSEPHSON: That's correct. That's what we have argued. And we think there's a lot of analytical overlap between the two. But if there's any doubt, any doubt about whether a particular charge, unreimbursed charge could somehow jump the Article III hurdle, it certainly would not jump the actual damage threshold.

The plain language of the Privacy Act says that a plaintiff must show monetary loss sustained by the individual. The plain language of the Act requires a personal showing of loss; not that a financial institution has borne the loss, not that the loss might be sustained at some future point. It's past -- a past showing of monetary harm. And that has not been done by any of the 38 plaintiffs.

THE COURT: Well, some of the plaintiffs allege actual unreimbursed out-of-pocket costs; having to pay fees to pay their bills in a certain way and doing the credit

monitoring services, or the time and effort involved in dealing with their credit card companies to deal with these problems. Are some of those enough to be an injury?

MR. JOSEPHSON: No, Your Honor, they're not. And as we've separated these categories in our briefing, I think it's important to analyze them in terms of time-spent allegations. We have to spend time reviewing our credit reports or our accounts. The problem with those allegations is they don't monetize any of the time. No plaintiff says I had to spend X amount of time and I had to take off work, I normally get paid X amount of dollars. The Privacy Act requires that kind of monetary showing. That has to be the allegation. So to the extent plaintiffs are claiming time, they would fail.

To the extent plaintiffs are claiming they have to take mitigation measures in order to prevent the future risk of harm, and there are various -- as you mentioned, various measures that they allege. Our first argument is that doesn't establish -- get over the Article III standing threshold under the *Clapper* analysis because the first question is would you have a certainly impending risk of harm? If the answer is no, doesn't matter what measures were taken, even if they're reasonable.

So all of -- categorically, all of the things that plaintiffs allege that they have done would fail to

establish standing because they haven't established a certain impending risk of harm.

There are two plaintiffs, an anonymous plaintiff, Jane Doe, and Charlene Oliver who allege that they have spent -- actually, if I may back up. There are also plaintiffs that allege fraudulent charges in various accounts, but they don't allege reimbursement of those accounts. As we've discussed earlier, that would not get over the actual damages threshold because there's no showing that the amount remains unreimbursed. So to the extent a particular charge itself is the actual damage, that allegation would fail unless they say we're liable for it.

There are two plaintiffs that allege they have spent money on credit repair services, which are -- they distinguish from credit monitoring services on the theory that credit repairs past-looking -- we have to spend money to fix things that have already happened, whereas credit monitoring just gives us information in order to evaluate if something may happen in the future. But those two plaintiffs still would fail, we argue, fail the Article III standing test, as well as the actual damages test because they don't connect any of the underlying fraud that they claim they had to fix to this incident.

So any of the expenses that they've made, that they allege they've had to make to fix the fraud won't be

caused by this cybersecurity incident.

THE COURT: Well, before I started asking you questions about the breach, you were talking about whether a breach is targeted or not and you were differentiating people who steal private information on purpose from people who stole a laptop out of a car and, oh, my God, it had all this private information on it. But if it's relevant that they stole it on purpose, is there a further differentiation between people who stole it for financial reasons and people who stole it for other reasons?

MR. JOSEPHSON: That -- yeah, that's absolutely a factor in the analysis. And it goes to the speculative nature of the harm. To say that a breach is targeted generally doesn't really show that there's an imminent threat of a particular type of harm. The whole question is does --

THE COURT: So you're basically standing on the fact that it's not alleged that it was targeted for this purpose, and there's no facts in the complaint that support that it was targeted for this purpose, and that negates the notion that there is a risk of this. But I'm not supposed to look at what the purpose might have been?

MR. JOSEPHSON: I think that's a fair assessment.

THE COURT: And no one in -- I mean, I understand that the administration has been very careful about not

making certain statements publicly, but are you telling me that no one in the administration, not the director of National Intelligence or anyone else has attributed this breach to a foreign intelligence effort that is not official in any way?

MR. JOSEPHSON: Well, Your Honor, the -- again, I would say two things. The first is that we take the allegations in the complaint, we think that that -- those are the pertinent facts before the Court and they require dismissal of the case. The facts as pled require dismissal of the case. There's -- the investigation is ongoing into the incident. I'm not prepared today to comment on its status. But I think that when you look at the allegations of the complaint, they're insufficient both on Article III grounds and for the Privacy Act actual damages issue.

THE COURT: Is there any other point you want to make related to those issues for standing and the Privacy Act damages before I hear from the plaintiffs on those particular issues?

MR. JOSEPHSON: Yes, Your Honor. Just quickly two points. One, in addition to emphasizing the targeted nature of the theft, the plaintiffs have also emphasized the fact that they've alleged past misuse in an effort to show that future misuse isn't speculative. There's three problems with that, though.

The first is the misuse that they've alleged is comparatively minimal. We have a significant number of plaintiffs, 18 plaintiffs who do not allege that anything has happened to them at all. It's all about future risk; 18 of the 38. That is a significant amount of plaintiffs.

The second issue is they never connect the past harm to this incident. So, they certainly can't rely on the past harm to show that future harm is imminent. And the final thing I would say is there's been no indicia of repetition. There's been no showing, well, that past harm occurred so it might happen again. In fact, the contrary is true.

If fraud happens on a particular financial account number, generally the account number is canceled, as numerous courts have explained in data breach cases. And so the idea that that would -- again, it's not even traceable because there is no account number in the breach, but it's certainly not true that it would have happened again. So the past misuse, the attempt to piggyback on the past misuse to show imminent harm fails.

The other point I would make is there's been much ado about credit monitoring services in this case, which is interesting because the government has already provided those services for a decade. So to the extent plaintiffs are trying to recover those costs, they've already been

provided, and they've never really had a good answer other than to say, well, we might have to buy them when the decade runs out, we may have to buy them in year 11.

But whether or not a particular plaintiff decides to purchase a service in 2025, you cannot plausibly say that that expense is linked to this incident. That is a decision that that plaintiff may make based on their own personal credit profile and where they're at at that point. But way too much will have happened in ten years to link it back, to link that charge back to OPM in this case.

THE COURT: Thank you. All right. Which of the plaintiffs' counsel is going to be dealing with standing?

MR. GIRARD: Good morning, Your Honor. The standing analysis here, I think, first of all, is worth recognizing that we're not talking about a data breach that fits neatly within the categories of cases that Courts have already adjudicated, primarily because here the core claim is the claim under the Privacy Act. And for purposes of standing, if you go through the elements of it -- as I understand the Privacy Act, it's really codifying common law privacy protection principles.

And, yes, in the *Cooper* case the Supreme Court said emotional distress damages are out and it has to be actual out-of-pocket damage. But for purposes of standing, I think the way the analysis has to go is that the release

itself is the injury, it's the adverse effect, both with respect to the safeguards claim and the claim for the unlawful release.

And in the *VA Laptops* case this issue was specifically considered and the Court said yes, that's an adverse effect, that gives rise to Article III standing. That opens the key to the courthouse door. Now, there's --

THE COURT: Where does -- where do you get the theory that the release itself, they opened the garage door, is in and of itself an injury in light of *Spokeo* or any of the other cases? That even if that is sufficiently concrete and particularized, how do you get the imminent harm, actual imminent harm? You're saying that just the loss of data alone in and of itself is not only concrete and particularized, but it's actual and imminent? And how does that fit in with Judge Alito's language calling for a material risk of harm, which seems very similar to the clearly impending language --

MR. GIRARD: So my answer is that this isn't like a procedural violation case because the harm has occurred upon the release, and the reason is that the underlying claim is rooted in the common law protection of privacy principles. And so it was recognized at common law that if your private information was made public or there was an intrusion upon your right to seclusion, the injury occurs at

that moment. And this is a precise issue that the Court looked at in the *VA Laptops* case. It's also been the position --

THE COURT: I think that's what Justice Thomas was saying in his concurrence a little bit in *Spokeo*, if the statute is vindicating a private right, that that's all you need, without more.

MR. GIRARD: Right. And so, yes -- so, in the way I see this, I don't think you get to the question of imminence because we're not talking about a risk of future injury; the injury happened.

There's still, of course, the question as to whether you have stated a claim in the sense that you've pled actual damage. But you have the right to be in court on that because we're not premising the Court's Article III standing on a risk of future injury, we're premising it on an injury that has occurred and has been recognized at common law. So it isn't like --

THE COURT: But doesn't that injury still have to cause harm? Isn't that what the majority opinion in *Spokeo* said?

MR. GIRARD: Yeah, and it does cause harm. And again, the harm is recognized at common law. So it's not like a situation -- let's say it's a Truth in Lending Act claim and you have the right to some disclosure and you

never saw the disclosure, you never got the mail, you never relied on it, it never had any impact on you whatsoever. That's *Spokeo*. This is different.

This is a common law right to the protection of your private facts. That right is infringed at the point when the release occurs. And the causation issue doesn't enter in because they've admitted, when they notified the people, that we, as the OPM, are telling you that your information was released from our control. And so there really isn't an issue.

And, I mean, I think it's pretty clear, standing has been established. Now we can go through the whole --

THE COURT: Well, it seems like you spent most of your brief arguing that standing was established through all these other things.

MR. GIRARD: Well, we were responding to those arguments. We're not going to let those go unanswered.

THE COURT: Let me ask you this: Even if I read *Spokeo* to say that Congress specifically created a private right of action for a violation of private rights in the Privacy Act, wouldn't that only relate to the Privacy Act claims under the provisions invoked here, which can only work in cases of actual damages? How would that help with your APA claim for injunctive relief, which is predicated on OPM's violation of FISMA? On what basis could I possibly

conclude that that statutory regime was specifically intended to vindicate private rights?

MR. GIRARD: I guess that goes to a broader question of whether you go through standing on a claim-by-claim basis.

THE COURT: Yes, you do. Yes, you do.

MR. GIRARD: I guess that's the answer.

THE COURT: Do you have any case law that tells me I don't?

MR. GIRARD: I always thought -- I think the law of standing has evolved quite a bit, you know, at least in the time since I've been a lawyer. I thought standing was a gatekeeping doctrine that says, Do you have a right to be in court? You know, under the *Lujan* case, for example, to me, once you're in court, if you read cases, Courts don't go through every claim and every defendant in the case and analyze standing separately for each one.

THE COURT: But you're asking for declaratory and injunctive relief. If I don't have the power to give it to you because you don't have standing to ask for it and the only claim you have standing to bring is the Privacy Act claim, how can I ignore that?

MR. GIRARD: Let's back up then. Let me answer your question directly as to that.

THE COURT: Okay.

MR. GIRARD: So if the argument is that there's not enough imminence to support a claim for injunctive relief under the Administrative Procedure Act, our response is that's a fact question and if you look at this -- this agency, by all accounts--and that's pled in some detail in our complaint--is still not adequately functioning to protect information. And the imminence that we have to show isn't that we're going to be the -- our clients are going to be the subject of some targeted theft in the future, the imminence is that there's a likelihood of a further breach causing the same harm that's already been caused to them.

THE COURT: Right. But what you're saying is that Congress, in the Privacy Act, took people's privacy rights and statutorily created a private right of action. But in that statute it specifically said it's only for damages and it's only for actual damages and it only goes up to $1,000 a person, no declaratory and injunctive relief. So how does that get you to the APA count?

MR. GIRARD: Well, I think that the argument is that the Court, under the APA, has the power to enforce the obligations of the agency to take the necessary measures to protect their private information, that it's really the claim of last resort when there's no alternative from the perspective of the class members to vindicate those rights.

THE COURT: What's your best case for the

proposition that the loss of private information, the revelation of private information in and of itself, without -- just that sort of inchoate harm is an Article III injury in fact?

MR. GIRARD: I guess I would refer you to the decision in -- I've mentioned the *VA Laptops* case several times, with the District Court opinion. I think the same principle is in *Doe versus Chao*, that the release itself is itself an injury. And if you think about it, I mean, it -- the other point we cited in our papers --

THE COURT: A lot of those cases are all pre-*Clapper* and pre-*Spokeo*. And once you get to *Clapper*, what's left of that argument?

MR. GIRARD: Well, *Clapper* is talking about a situation that we think is really distinguishable in the data breach context.

THE COURT: It seems like it's the most similar because it's intelligence information, it's not credit card information. Almost all your cases are about credit cards.

MR. GIRARD: And they moved and they cited to credit card cases. There aren't a lot of analogous cases in the data breach context. I guess the point I want to make with *Clapper*, *Clapper* is really more analogous to the cases like the *SAIC* case where you have what I think of as a smash-and-grab theft of a laptop out of the back of a car

and you need a speculative chain of events in order to result in some harm to the plaintiff who's suing.

This is a different situation here because we're not premising the Court's jurisdiction to hear this case on a speculative chain of events. The harm has occurred. They've all been told that their information is in the hands of hostile persons or persons that are ill-intentioned.

You asked about the nature of this hack --

THE COURT: They've been told that it's gone. I don't think they've been told anything about the intentions of the people hanging onto it.

MR. GIRARD: What the defendants -- the government calls it a sophisticated and malicious hack and they acknowledge the information was exfiltrated.

I want to answer the question you asked about who the actors are behind this and the speculation on that and how the Court should look at that. I mean, I guess, you know, we interviewed our clients, we tried to screen for what I think of as false positives in the sense of people who would say, oh, no, I've gotten notified of five other data breaches this year, and those are aren't the people in the complaint. These are the people who told us this is new, and in some cases there's no other way they could have had this information.

And this I'm offering really based on media

reports. I'm not testifying to this as a fact witness. But the investigation that we've done, there are media reports that link the source of this hack to hacks conducted by a group that is apparently connected to other hacks, including Anthem, which is a health care company, supposedly Permira, and possibly a hack of United Airlines. There's also speculation that this group has monetized the information. It's not like, you know --

THE COURT: I really don't know what to do with all this, it's completely outside of the record.

MR. GIRARD: Well, you asked about it and so I'm answering it. And to the sense you're going outside of the record --

THE COURT: You just cited *Doe versus Chao* to me, which is 2004 case, pre-*Clapper*, and in that case the Supreme Court held the plaintiffs must suffer actual damages to be entitled to the statutory guarantee under the Privacy Act. They don't address standing. So how is that a standing case?

MR. GIRARD: Let's go back to *Clapper* then. In the sense that *Clapper* is talking about a speculative chain of events, the Court in the *Adobe* case and in the *Remijas* case addressed this argument about whether *Clapper* should be applied to data breach cases like this one and rejected that argument because the issues really aren't the same. Let me

give you a concrete example.

So we have individual plaintiffs who are notified of the data breach or had already experienced incidents of identity theft and had the reaction that they wanted to buy credit protection. The government announced, I believe it was in June, that the hack had occurred. Their credit protection wasn't up and running until September.

Somebody who bought credit insurance in response to that announcement, to me, is someone acting reasonably. And even if you conclude that -- that question of reasonableness is determined as of the time the person acts. It's not determined with the benefit of hindsight. And to say, when the government has already admitted that they spent something like $160 million as of the time these papers were filed on credit monitoring, for them to say that that's an unreasonable thing for an individual to do, I don't know how they get to that. And --

THE COURT: Well, if they're paying for it, why is it a loss for the individuals? Why would they have to pay for it?

MR. GIRARD: Someone who buys it before the government puts their credit monitoring in place, how is that an unreasonable expenditure? My contention is it's very difficult to attack that on any level as being anything other than a cautious reaction to an announcement of this

nature. And that person has pled a claim and is entitled to be before this Court and passes all of the checks of Article III standing and everything else.

Then, you know, you take separately under the Privacy Act the claims for the people that have --

THE COURT: Well, I asked you what's your best case for the notion that it passes muster for Article III standing and you pointed me to a case that doesn't talk about Article III standing, *Doe versus Chao*. So tell me, what's your best case for the idea that the private information is gone, that's it, you're done, no need to prove material risk of harm, clearly impending harm, financial loss, reasonable fear of harm, it's gone, the barn door is open, standing. And that's appealing because certainly everybody whose data is gone feels like they were hurt by the breach. I'm not trying to diminish people's feelings about it, I'm trying to figure out how it fits into Article III constitutional standing.

MR. GIRARD: The dissent in *Doe versus Chao* --

THE COURT: Basically you're saying something bad happens. And I just don't know if there's a case that says something bad happens equals standing.

MR. PATTERSON: Well, I wanted to address the *Doe versus Chao* case because in that case the Court addressed the merits, what was required for actual damages. The only

injury alleged there was emotional distress. And Justice Ginsburg, in her dissent, said *Doe* has standing to sue, the Court agrees, based on the allegations that he was torn all to pieces and greatly concerned and worried because of the disclosure of his Social Security number and its potentially devastating consequence.

THE COURT: And she said that, though, before the Court later issued the *Clapper* opinion. So, I don't know what I can -- emphasis I can put on her dissent there. I mean, it's clear from her dissent in the *Spokeo* case that they thought particularized was -- she, and I think it was Justice Sotomayor joined with her, that particularized got you to concrete. But I don't think that even they said particularized and concrete got you to actual and imminent and not conjectural.

MR. PATTERSON: Well, and in the *Cooper* case emotional distress was the only thing at issue there, too. The Court went on to address the merits, so everyone understood the plaintiffs had standing. In this case it's different from *Clapper* because *Clapper* --

THE COURT: So if you have standing but you get -- if your emotional distress is because my information is gone, if I agree with you, that will give you standing, what good does it do? And don't I still have to throw the case out if it doesn't give you a Privacy Act violation?

MR. PATTERSON: Not against KeyPoint. And against the government, our plaintiffs have, many of them, alleged actual monetary damages.

THE COURT: All right. Well, then I think we need to talk about causation there. But, most of the cases you cite of connecting the harm or saying that the fear of future harm is sufficient to be an injury are cases like *Neiman Marcus* and -- I don't know if it's *Galaria* or *Galaria* case, but why is this case more like them than like *Clapper*?

In *Galaria* the Court drew the reasonable inference from the fact that it was a domestic criminal theft of personal information from an insurance company, was for the very fraudulent purpose alleged in the complaint. Do you even allege in your complaint that this breach was undertaken to advance financial fraud or identity theft?

MR. GIRARD: We didn't allege that.

THE COURT: Any purpose?

MR. GIRARD: We allege the identity theft incidents and allege the correlation between how those happened in time and the nature of the information that was used.

THE COURT: Well, the correlation allegation that I saw in your complaint was "thereafter," which you improved in your motion, your opposition to the motion to dismiss, to "consequently." But I don't see any facts that alleged a

correlation. Where in your complaint do you allege a correlation?

MR. GIRARD: So the correlation is in each case that the misuse of the data occurred in time shortly after the breaches occurred, so --

THE COURT: Shortly after being notified of the breach?

MR. GIRARD: No, in some cases it happened before the notification occurred but after the breaches, after we now know the breaches occurred. And we've also pointed to the correlation between -- for example, with a --

THE COURT: Is chronology enough to establish --

MR. GIRARD: No, it's not. And so what the Courts have looked at is both chronology and whether the theft is one that is commensurate with the type of information that was stolen. So --

THE COURT: So where do you allege anywhere in your complaint that credit card information was stolen?

MR. GIRARD: So, to answer that question specifically, we alleged in the complaint that the information stolen included information like financial accounts. And they've fixated or focused on the information that's included in the SF-86. And in some cases just -- specific paragraph where this appears is paragraph 144 and paragraph 146, information about financial accounts, debts,

bankruptcy filings, credit ratings and reports.

THE COURT: Correct. But that's very vague and it's summary. I went over the complaint with a fine-toothed comb and tried to find any allegations that support the causation requirement. In paragraph 7 you said plaintiffs have suffered sustained economic harm from the misuse of stolen information, which is conclusory. Paragraph 10, you said sensitive information stolen includes, at a minimum, Social Security numbers and date of birth. Paragraph 13, you said the SF-86s contained sensitive information. And you state in your individual plaintiff allegations that numerous plaintiffs completed the SF-86 and at least one the SF-85. So I take it I consider those for purposes of this motion, what they ask for, right? I have to.

MR. GIRARD: Yes. Right.

THE COURT: Okay. So, you allege in paragraph 67 that the SF-86 contains Social Security number, date of birth, and, quote, financial histories and investment information. That still doesn't zero in on the notion that the forms contain the kind of information the plaintiffs say is being misused. Paragraph 68 talks about an SF-85, but doesn't tell me what it asks for. Paragraph 74 says the electronic official personnel folder contains a birth certificate, employment history, Social Security number, date of birth. Paragraph 144 that you just pointed to said

that the highly sensitive personal information stolen includes, quote, financial and investment records.

So, nothing in the complaint alleges that either the SF-86 or the SF-85 calls for credit card numbers, debit card numbers or bank account numbers.

You also allege that, paragraph 146, that job application forms include, quote, bank account and credit card information, but you don't describe the information.

So there is not a single allegation in the complaint that a single plaintiff who suffered credit or debit card or bank account misuse gave that information, the credit card or the debit card, the bank account to the government. If you're tying the harms, those particular harms to the SF-86, I went through the entire SF-86. It asks for what -- well, the first 62 pages don't even mention finances. Page 63, they ask, tell us about your foreign investments; 73, foreign business activities; 100, explain if alcohol or drug use has had a negative impact on your finances; 106, have you ever filed for bankruptcy; 107, financial problems due to gambling losses, failure to pay taxes.

So, yes, they call for financial information, but not debit card numbers, credit card numbers, bank account numbers. And I don't need to read you the whole thing, you've read it. It isn't until you get to the very end

where they say, have you ever had any credit cards canceled for default, give me the account number, did they ask for an account number. And clearly that's not the one that these people are having these problems with now. So, what's the link?

MR. GIRARD: Yeah, so let's start with the tax returns. So --

THE COURT: Well, they said that they're not -- well, they are going for causation with the tax returns.

MR. GIRARD: And so with the tax returns --

THE COURT: You need a Social Security number.

MR. GIRARD: You need a Social Security number, a date of birth, and the name of the individual, and that information is clearly disclosed.

THE COURT: Okay. So you got the first link in the chain.

MR. GIRARD: Right. Okay.

THE COURT: And we'll go to the rest of the chain. But with respect to the credit card people, the 15 people that you're relying on as plaintiffs who suffered an injury in fact, what's the first link? Is there any allegation in your complaint? Did I miss something that said a single one of these people gave that information to the government?

MR. GIRARD: So the reason that's in there is when we interviewed these people, they told us they're convinced

they gave this information to the government in other context.

THE COURT: You didn't even allege that.

MR. GIRARD: Well, we allege generally that they provided this type of information to the government.

THE COURT: No, you said they filled out the SF-86, they filled out job applications. Nowhere did you say they gave credit card information, debit card information.

MR. GIRARD: You're right about that. I don't dispute that we didn't say they gave credit card information. So, the way Courts have dealt with this, Courts have used this to say that, for example, if you alleged a fraudulent tax return was filed in your name but the hack only involved credit card data, that you couldn't get from point A to point B. So it's been a screening device.

THE COURT: We're trying to get from point A to point B. How is that -- it doesn't work.

MR. GIRARD: My answer, the answer I can give you is that Courts have been fairly generous in recognizing that when you have much less data than was stolen here, that it can be misused to get to a person's identity and commit identity theft.

My understanding, for example, with a debit card is that you can put charges on someone's debit card if you can get to the name of the account. Simply the account number. You don't need the pin, for example. And so in no

case that I'm aware of has a Court, confronted with --

THE COURT: Someone committed a sophisticated, malicious, organized attack on the entire federal government and took 22.1 million people's personal data and somehow then, we don't even know if it was encrypted or whatever, they were able to pull out of it someone's information and then reverse engineered that and managed to get it to a single human being in the United States who maybe went to charge something to one person's debit card? How many links in the chain there are completely speculative and hypothetical.

MR. GIRARD: There is -- in any data breach case where you're stealing the data to misuse it there's going to be a chain like that and --

THE COURT: Right, and that's why a lot of them say no standing. And the ones that do find standing focus on the fact that the theft was for the very kind of information that's being misused. That's what *Neiman Marcus* said. Why else would they want this information? That's what they said in *Galaria*. That's my problem here. What is it that connects this breach of the scope and the nature that we're talking about and the kind of information that was even in there, now you're saying they took it and somehow got to information that wasn't in there. Why is that a reasonable inference from the face of your complaint?

MR. GIRARD: The -- all I can do is speak by

reference to the case law. I can answer the question directly factually, which is we interviewed these people, they believe the proximity in time and the nature of the information is connected. It's possible, I think, that in discovery not all of these incidents would turn out to be connected, some they could probably disprove.

What Courts have said, confronted with these facts, is they've recognized the limited information available to the pleading party. They've recognized the principle that in situations where it's possible you have multiple wrongdoers, that the burden shifts to the wrongdoers to disprove their responsibility, citing the old cases of *Summers versus Tice*, which was cited in the *Remijas* case.

THE COURT: Well, again, just the fact that your 15 incidents of credit card irregularities are entirely different, different types of cards, different stores, different amounts, different states, different timing suggests that they're entirely unrelated to each other and, therefore, unrelated to the breach.

MR. GIRARD: It could be that some are related, some aren't. It could be that the information was sold and monetized in different ways by different people at different times; it could be that the defendants are right and they're unconnected. But we're talking here about standing and at

this stage --

THE COURT: When you said it could be, could be, could be, and the standing test from the Supreme Court says not conjectural or hypothetical, aren't we done?

MR. GIRARD: I don't think we're done because those are situations that didn't involve injuries that were actually pled. Those are situations where the Court is talking about an injury that might happen in the future, when there's been no misuse alleged. So that's the distinction I would draw.

But let me offer this as an alternative. Let's say that you were to conclude that these are too attenuated and that we haven't drawn enough of a connection and we shouldn't even be allowed to re-plead. I would say in passing, I mean, I think you're reaching a factual conclusion that's premature, which is that the purpose of the hack was intelligence only and that the information -- you know, the hacker signed a confidentiality agreement with Chinese government not to use it for any other purpose. I'm not sure that's how it works. I don't think --

THE COURT: I don't know what the purpose of the hack was. I know what's been publicly reported. You have the burden to allege facts. What they're saying is they're not even relying on it. They're saying your allegation that there was any desire to commit identity theft or financial

theft or financial fraud, that that underlies this breach, it's absent, it's not in the complaint. You don't allege it.

MR. GIRARD: And so I guess my response to that is we have alleged specific incidents that are connected in time and in the manner misused, which is consistent with other cases like *Anthem* and *Permira* and *Target* that have allowed these cases to proceed past the pleading stage. And true, this is a different type of breach. But let's --

THE COURT: What connection is there other than timing?

MR. GIRARD: Well, in the case of the tax returns, there's the fact that the information misused was Social Security number information, which they had. And, you know, my understanding, the government announced they have a call center that's been running to handle communications from the people affected by this breach. You know, if we move forward, we get access to discovery, we'll be able to find what they've been hearing from the rest of the people out there that are affected.

I mean, you know, we're pleading a small subsection. We're pleading a group that we think is representative of the types of complaints out there that people have identified and what they think happened. You know, there are broader sources of facts out here to get to the bottom of it, but --

THE COURT: Has the existence of this lawsuit and your availability to hear from people who have had things happen to them been broadly advertised to the class?

MR. GIRARD: No, no.

THE COURT: Certainly within the union, they know.

MR. GIRARD: The union knows, but it's not -- you know, we haven't put out a general call.

But let's talk about other incidents. Let's say you hypothetically thought that the connection between the credit card invasions or debit card charges was a connection you weren't willing to accept, you would still have a complaint that in a number of cases alleges people bought identity theft protection, and there's a fact issue of whether that was reasonable or not, it certainly constitutes injury. They can say, oh, well, it's too speculative, and out of the other side of their mouth they can say, you know, you should have been satisfied with the product we bought you.

THE COURT: Doesn't *Clapper* take care of that? I mean, how does that -- doesn't that say I'm not supposed to look at that as an injury?

MR. GIRARD: No, because *Clapper* is talking about whether somebody was subject to electronic surveillance by the federal government without having a basis to say they were specifically being targeted. This is a different situation where the government itself has announced your

information is in hostile hands, you should do preventive things, including monitor your credit. And so for someone to react to that and say, oh, my God, I'm going to buy credit insurance right now, when the inquiry is based on is it reasonable at the time, I -- I have difficulty seeing how that's an unreasonable thing to do. Separately --

THE COURT: What's the case that says -- that you keep quoting, was the purchase reasonable at the time?

MR. GIRARD: You know, I'm going to have to -- if we have a break at some point I'll answer that question specifically in terms of the --

THE COURT: Because you've given me that formulation a number of times.

MR. GIRARD: And the issue is when a Court looks at a remedial measure, do you look at it after the fact, with the benefit of knowing what ultimately happens, or do you look at it, the decision the person makes at the time they do it? Separately you have a number of other expenditures.

Let me give you another example. Someone who puts in a credit freeze on their account as a reasonable reaction to this, it's one of the things that's repeatedly recommended as a reaction to a data breach, then pays a charge to lift that credit freeze, you know, again, these are expenditures that the Privacy Act contemplates are going

to be the types of things people are going to be able to claim.

In the wake of the *Cooper* decision, since emotional distress is out, if you read the dissent in *Cooper*, what they're saying is, in effect, all you've left are relatively modest expenses. And these are the exact types of things that we think are going to be at issue for the purpose of these Privacy Act claims. It's things like somebody who bought credit insurance during the intervening period, somebody who paid to lift a credit freeze, somebody who paid a credit repair firm, for example, if they can show the factual connection.

And so, I think if you look at the range of incidents that we pled, it's clear that even if you were to conclude that from a factual perspective you're not going to accept the correlation between this hack and the credit card or debit card overcharges, I don't know how you disregard the fraudulent tax return filings based on the case law. But, even if you did that, there would still be other claims that are compensable, like the ones I mentioned.

THE COURT: Well, even if you've got fraudulent tax returns, as I said, the first link in the chain, my Social Security number was stolen and a Social Security number was needed to do this, is that enough to get you all the way to this breach is why there was a fraudulent tax

return? And how were they financially harmed by the fraudulent tax return?

MR. GIRARD: So to answer that question, is this enough? depends at what stage we're talking. If we're talking about standing, yes; if we're talking about motion to dismiss, yes; if we're talking about summary judgment or trial, no.

And is it enough -- it's what every other case out there has required. There's -- no Court has said you have to somehow correlate the hack with -- in some factual way beyond pointing to the correlation between the theft of the data and the misuse. I mean, it -- again, the factual details about where --

THE COURT: Aren't there other cases that go the other way?

MR. GIRARD: There are cases that, I think, if you look at them -- I mean, the decision I thought was interesting was the *Kahn* decision, K-A-H-N, that says if you look at all these, they seem to line up in two categories. There are ones where the Court found the allegations -- there was -- in a number of those they're the ones that involve the theft of a laptop or, you know, somebody loses the data tapes or something like that. And those, I agree, they lend themselves to a *Clapper*-type analysis because you have to assume that the person is going to have the hardware

and the software to go upload the data and then de-encrypt it and then have the intention to misuse it, etcetera, etcetera, and you really have a speculative chain.

The other type of cases you have are cases where there's a breach and somebody takes a plaintiff who alleges a fear of future injury alone and points to the breach. And Courts have had a lot of trouble with those cases as a matter of standing. And I think it's a mistake to try to fit this case into those facts because there's no case that involves the theft, the exfiltration of information that is as comprehensive as this case is.

And I think when you're looking at what is a reasonable reaction to this, you really have to take into account the exceedingly private nature of the information that was stolen and the gravity with which the federal government reacted to this, and appropriately so. And when --

THE COURT: You're answering a different question. I'm talking about if you got fraudulent tax returns, my Social Security number was stolen, my Social Security number was used, and you're saying that's enough, even though the number of steps in between is completely unknown, conjectural and hypothetical, that's enough for now for standing, even though it might get thrown out later. I'm asking you, where does that get you? What financial harm is associated with the filing of a fraudulent tax return?

MR. GIRARD: So with respect to our clients, and here I'm updating to some extent, so let's assume -- in at least one case our client is still waiting for the refund, the identity theft incident hasn't been resolved. In other cases it's been resolved; one person got interest, other people didn't. So there's potentially a claim for interest where it wasn't paid. Maybe that's a claim against the IRS; that's a factual issue they can raise.

But in all these cases there is a tremendous amount of time put into unraveling those problems. If you get past the causation hurdle, then that time becomes compensable under the Privacy Act.

THE COURT: Time is compensable under the Privacy Act?

MR. GIRARD: Yeah. And this was an issue that was addressed in the *Bivens* case. It was addressed more recently by Judge Gottschall in a decision called *Makowski*, if I'm pronouncing that right, where the Court assumed that time could be compensable under the Privacy Act. They argue it has to be pled with greater specificity, we say what we've pled is sufficient at this stage.

THE COURT: What's your causation allegation in connect with KeyPoint? You say hackers accessed OPM with stolen KeyPoint credentials. How does that trace plaintiffs' injury to KeyPoint?

MR. GIRARD: So, what -- KeyPoint has really rested a lot of their argument on causation. What we've alleged against KeyPoint is that they were negligent in training their personnel, that the hack that resulted in --

THE COURT: What paragraph?

MR. GIRARD: Just a second.

If you look at the negligence claim asserted against KeyPoint, that is the most fulsome explanation at paragraphs 217 through 228.

And I'm not going to read it into the record, but we allege in some detail an overall negligent course of conduct. The most salient aspects of it are the failure to adequately train their personnel. What happened, as we understand it, is in 2013, in December, one of their employees fell for a really basic phishing scam and gave up their login credentials, that that act led to the subsequent exfiltrations that occurred in May and December 2014, that this was known within OPM and KeyPoint and that no action was taken to stop that theft in its course.

The period of time in which the hackers were in the company and for a period of time being -- not company, the -- within the KeyPoint and OPM date bases ranged over a period of months, and they were apparently under observation for a period of time and no action was being taken to arrest that hack in progress. And so we're saying that they're a

coequal actor with OPM.

These databases exist for the purpose of retrieving information and they know that if they're not secured, they're going to be misused. The -- I mean, it's important to understand the --

THE COURT: But can all that's in the complaint connect this somehow, what happened at OPM, to KeyPoint? I mean, what I see in the complaint is that there's an allegation about KeyPoint, but I don't see -- you're saying that the loss of the data by all these people in and of itself is enough to establish that there's standing to sue the government, but I don't understand what you're saying gives them standing to sue KeyPoint.

MR. GIRARD: The -- we've pled that KeyPoint is liable for negligence in the way that it maintained its database. The fact that it -- it is at the source of the hack that led to the exfiltration of all the data that creates the injury to our clients.

THE COURT: Well, you said the hackers accessed OPM with stolen KeyPoint credentials. But do you actually allege that what was taken in the KeyPoint hack actually facilitated the OPM hack in the complaint?

MR. GIRARD: Yes.

THE COURT: You're telling me that.

MR. GIRARD: Yes.

THE COURT: And that's all in the negligence part?

MR. GIRARD: No. It's in the description of the hacks at paragraphs 127 through 133 before we describe this. And, you know, we've talked -- I mean, this is an area -- we think what we pled is sufficient because we're pleading negligence. We're not pleading under a particularity standard here, under 9 -- 9(b) standard. But, this is an area where if the Court thought more detail was needed, we would ask for leave to amend because there's a lot more information out there now than when we pled this.

But again, we think that what we've pled is sufficient because we pled that the source of the hack goes back to KeyPoint and their failure to use adequate measures, as we've alleged in greater detail in our negligence count and in the paragraphs I cited, to protect access to the network. These two networks were linked and so any breach on the KeyPoint side meant that you got into the entirety of the OPM site.

THE COURT: All right. Is there anything else you want to tell me about the standing issue right now?

MR. GIRARD: I mean, I think that's it. I guess the -- the one point that I'm not sure I was as clear as I would like to be is I don't think just trying to take *Clapper* and apply it to these facts really works because I don't think this is the same as *Clapper* in the sense -- I

think *Clapper* makes sense when you're applying it to a situation where you have a laptop that's stolen.

This is a situation where you have information that has admittedly been released, that release is a -- you know, if you think of it in a common law sense as an intrusion upon private facts, I think the somewhat archaic term, that's a wrong, that's an injury. That's an injury that's been suffered by each member of the class. The Privacy Act recognizes and codifies that as a wrong and that means we have the right to be in court. Beyond that --

THE COURT: So really, the whole discussion in both briefs about the credit card stuff, the tax returns, the fear of future harm, the emotional distress was completely unnecessary because the fact of the breach is an injury. Did you even argue that in your opposition?

MR. GIRARD: I think we did, but it just occurred to me as I was reading, I don't think it's lost work in the sense that I think we have to analyze it. I mean, you know, this all comes up in the context of the actual damages claims and those are fair game. I mean, you told us to be prepared to argue those, so I think, you know, that's what we're doing.

But I think for the, you know, very limited purpose of Article III standing, I think it makes sense to look at the case that way under the Privacy Act, and that's

just a function of the fact that the other data breach cases weren't brought under a statute that is analogous to the Privacy Act.

THE COURT: Okay. But that, I think I'm just -- I've already asked you this question, I don't see how that helps you with count -- with the APA count.

MR. GIRARD: Well, I guess the --

THE COURT: Unless you just -- once you're in the door you get to bring whatever you want?

MR. GIRARD: Not whatever you want, I mean --

THE COURT: All your other claims, like attendant subject matter jurisdiction theory?

MR. GIRARD: I mean, I guess I -- I don't think the issue of Article III standing is really subject matter jurisdiction. I think it's simply do you have the right to be in court at all, binary, yes or no. It doesn't mean you have a claim. All the other defenses apply. But I just, when I think about it, I just think it's a creature of --

THE COURT: Standing is a prerequisite for subject matter jurisdiction.

MR. GIRARD: Of course. But it's linear. You start with standing and then you go to subject matter jurisdiction. So you could throw the case out for any one of, you know, 150 reasons once you find standing, but standing is just inherently very limited.

But, I mean, at this point, it's just an observation, but if standing is being used in ways -- if it was meant to be applied to each and every defendant in each and every claim, all the decisions we read would go through it each and every time; they don't. Once it comes up as --

THE COURT: Well, as most of these cases are APA cases, there's not a separate statutory claim, like here you have Privacy Act and APA. So, that's why they don't look at it with -- I mean, almost every standing case I've ever had has just been an APA case that implicates a violation of some other federal statute.

MR. GIRARD: But so even, if you weren't buying my Privacy Act argument and the notion of the release itself as adverse effect, I think I've pointed to specific situations that involve out-of-pocket loss, like purchases of credit monitoring, payment to lift a credit freeze and the like, that they don't have an answer for that are cognizable and they have fact based arguments as, oh, you shouldn't have spent the money or it wasn't reasonable or something. But those are, I think, really not, you know -- certainly not standing and not even motion to dismiss arguments.

I understand your skepticism, as I perceive it, on the issue of the correlation between the credit card fraud and the debit card fraud. If you find that, I think you should acknowledge, at least for pleading purposes, the tax

return misuse and the expenditures associated with that.

And so thank you for hearing me.

THE COURT: All right. Thank you.

Go ahead.

MR. PATTERSON: Is it all right? I just wanted to answer a few points that you had asked here.

So, one, on the APA, I mean, I think it's really under *Lyons*, under equitable relief, that was the case where the person got put in a choke hold and was saying, you know, I'm going to get put in a choke hold again, and is that speculative or not? And here we're saying the same problems that led to the initial beach are still in place, so this is going to get hacked again. There are millions of hack attempts on OPM and so we're at imminent risk of this data getting breached again, and that's why we have standing under --

THE COURT: But I just don't have general equitable authority to tell the federal government what to do, absent --

MR. PATTERSON: Well, you have the APA, which gives you authority to tell the federal government to obey the law; the law, the Privacy Act and FISMA, the laws that we are arguing they're violating by not securing this information.

THE COURT: That goes to the merits of your --

MR. PATTERSON: Right. Yes, yes.

THE COURT: -- APA claim, which may or may not be correct.

MR. PATTERSON: Right. But in terms of standing, the imminent threat that this information is going to get hacked again because they have not fixed the problems that we identified in the complaint --

THE COURT: You're deriving your standing from the Privacy Act and the release of the information. And if that's a statute --

MR. PATTERSON: Right.

THE COURT: -- specifically doesn't give rise to equitable remedies. So I don't see how you can say I can import an equitable standing to grant an equitable remedy into a statute that doesn't give me that authority.

MR. PATTERSON: Well, we're not saying that the Privacy Act gives you authority, we're saying the APA does in terms of the equitable relief, and the default under the APA is that you have authority. It's only if you look to another statute and say Congress has taken that authority away. And this, again, gets to the merits of whether we have an APA claim, despite the Privacy Act.

But our submission is that the Privacy Act does not rid the Court of the authority it already has under the APA. And, you know, the Supreme Court in *Doe versus Chao*

acknowledged that that may be a possibility -- or it may have been *Cooper*, one of those two cases.

But two other points on distinguishing *Clapper* and where you said the reasonableness standing standard comes from is whether the mitigation effects were reasonable. *Clapper* distinguishes environmental harm cases. And this is from part IV.A. of the opinion. Is says because the unlawful discharges of pollutants were concededly ongoing, the only issue is whether nearby residents who are members of the organizational plaintiffs acted reasonably in refraining from using the polluted area. And then, again, they say the sole dispute concerned the reasonableness of respondent's preventive measures.

THE COURT: All right. It's *Clapper* and the cases that it cites that you want me to look at for that.

MR. PATTERSON: Right, for the reasonableness.

And finally, on causation, *SAIC*, which as you know is quite strict on standing, actually allowed one plaintiff to go through because he said an account, fraudulent account application was tried to open in his name, which would have required a Social Security number. And the Court said, while Social Security numbers were on these backup tapes, which as was stated earlier in the opinion, it was doubtful that the thief even knew what they were. But the Court said that was good enough for standing at the pleading stage.

THE COURT: And that claim, as I understand it, evaporated shortly thereafter.

MR. PATTERSON: Well, it did survive standing.

THE COURT: All right. Thank you.

I do want to talk about government contractor immunity. But I, before we leave this, want to give the government a very brief opportunity to -- and I will ask you, Mr. Warin, I'll just have you get up once to talk about standing and then move right into government contractor immunity. So I know you're here and I know you object on standing grounds as well. But I just -- I want the government to address the two specific points that they've focused on here.

Number one is that there has been a harm, people gave their private information to the government and the government has told them its gone. So how can that not be an injury in and of itself, without establishing further harm? Putting aside whether it gets you to the Privacy Act, does it get you in the door?

And then second of all, why, if you told everybody credit -- here are these credit monitoring things we're going to help you with, sign up, this is a big problem, this data is gone so we're offering you this thing, why their going out and buying it doesn't count as an expense that makes this injury real and that gets them into the Privacy

Act, too.

MR. JOSEPHSON: On the first question, the instant injury theory, that the injury occurred the moment the data was breached, that's been soundly rejected by numerous counts. And I would point the Court to the *SAIC* opinion itself which addresses that issue, the *Reilly* case in the Third Circuit, and also the *Zappos* case which we cite in our papers.

And the Courts generally reasoned that the instant -- just the loss of data, without allegations that it's been misused, does not constitute a concrete injury or an imminent injury as those terms have been defined in the Article III cases.

THE COURT: And *Spokeo* kind of left it hanging without really answering it, said it -- it didn't say just invasion of privacy, it kind of said the violation plus a material risk of harm gets you there, even if you didn't actually have any harm; they didn't define what that was. And if their response to that is you sent us a letter and said you need credit monitoring, why isn't that enough to allege a material risk of harm? And then when you take Justice Thomas' concurrence where he says if it's a private right, that's different than just a general public right, if somebody invades your private right, you have standing. And then you've got the dissenters saying we already thought

there was standing. If I'm counting heads, should I derive the conclusion that the Supreme Court would think there's standing in this case?

MR. JOSEPHSON: No, Your Honor. No, Your Honor, I don't think that's a fair reading of all the opinions. The question is when someone alleges that they've been injured because their information is out there somewhere, doesn't matter where, but they just know that it's not where it used to be, is that vague, ephemeral idea something that can be remedied in a federal court?

I think it's important to remember that these types of injuries are, unfortunately, prevalent in the digital age. This is something that happens a lot and so these gatekeeping questions are very, very important. Because when data breaches happen and an individual comes in and alleges that that company is responsible for a particular type of harm, it is incumbent upon them under Article III to allege some kind of connection between the two.

On the second question regarding credit monitoring services, the plaintiffs --

THE; COURT: Well, is my Social Security number was stolen, my Social Security number was used enough to allege the connection?

MR. JOSEPHSON: I don't think it --

THE COURT: You think it gets you injury, but it

doesn't get you causation?

MR. JOSEPHSON: That's correct. That's correct. For purposes of this motion we have not challenged the Social Security number misuse on injury in fact grounds. But it absolutely fails the causation analysis because the only thing they've alleged is that the Social Security number was subject to the breach and they happened to have Social Security -- a Social Security misuse incident post-breach. There's nothing else that would connect it, connect that misuse to this event.

On the credit monitoring issue, the plaintiffs have -- I want to first address the gap issue. Plaintiff -- the gap issue argument that the plaintiffs have sort of set forth. In their oral remarks the idea that between June and September somebody may have purchased services before the government offered the services and, therefore, that plaintiff may have a claim because they might have spent money before the government offered it, the first point is before you even analyze the mitigation measures, money spent, time spent, all these things that people are doing to protect themselves from a future harm, before that even arises, the first question is is there an imminent threat of harm? If the answer is no, as a matter of law those other expenses, those other things the plaintiffs allege that they have done do not constitute Article III injury. That's a

straightforward application of the *Clapper* framework. That's what Judge Boasberg --

THE COURT: What they're saying is if you're saying the harm is sufficiently imminent that we're giving everybody, 22 million people this protection if they're willing to type their Social Security number one more time into a computer, how can you stand and then turn around and say there's no imminent harm?

MR. JOSEPHSON: Two points. The first is the standard, the Article III standing standard is more stringent and it's different than simply saying a cost is reasonable. It has to be -- there must first be a certainly impending injury or a substantial risk of future injury. If the plaintiffs' allegations fail to establish that element, the costs don't matter, it's not -- not in the legal sense. It does not matter, it cannot -- a plaintiff cannot manufacture standing by choosing, even reasonably, to make a certain expenditure.

THE COURT: If it's a potential harm or a possible harm or a feared harm or even a reasonably feared harm, it doesn't matter unless it's a clearly impending harm?

MR. JOSEPHSON: That's right. Exactly right, Your Honor. And the second point I would say, the fact the government purchased the services means that plaintiffs don't need the services. You can't sue the government --

they sort of have glossed over that point. The plaintiffs do not need -- no plaintiff has alleged that the services offered are inadequate. In fact, they're quite comprehensive. And that hasn't been challenged in this particular case. And so to the extent that plaintiffs are saying they're damaged because they might have to buy the services, well, they've already been offered for at least ten years. And to the extent they're claiming that at year ten all of a sudden the expense kicks in and they have a claim, well, there's no causal connection in year 11 to this particular case.

THE COURT: All right. Let me hear from KeyPoint about standing and then we'll hear from KeyPoint about contractor immunity. Thank you.

My first question is is everything they said about standing applicable to KeyPoint? I realize you have additional arguments about things they haven't said about KeyPoint, but are all the other things that we've been discussing, whether just the mere opening the door is enough, those issues that affect you as well?

MR. WARIN: I think they do, Your Honor. But I -- and we obviously adopt the government's argument in large fold. But we're one click stop beyond the government. And I think the Court obviously has an extraordinary command of the complaint and the extra activities as well about the state actor phenomena here.

It's pretty clear here that when you look at the complaint it is bereft of allegations relating to KeyPoint. There are -- it's a grab bag of allegations, scattershot. And one of the things that we did, as the Court did, we went back and looked at the government form that is the genesis of this complaint and to try to link it up to the claims of these plaintiffs because obviously that's what the case law commands. There has to be a linkage there for injury in fact. And if the plaintiffs can't prove that, that is the gatekeeping function that this Court has under Article III. That's the standing requirement.

I heard plaintiffs' counsel's argument and, frankly, I thought that he essentially was saying, well, Judge, given all of this, you have to give us the benefit of the doubt. Well, that's precisely what the Supreme Court says you can't do, Your Honor.

THE COURT: Well, I think he's saying even if we lose on the credit and debit card fraud people, the Social Security number people are enough to get you standing because that information was on the SF-86.

MR. WARIN: It is. And indeed, it's on the bottom of every page of the form, through all 124 pages.

THE COURT: 127.

MR. WARIN: 127. Thank you, Your Honor.

So, you're precisely right that it's there, but

does that give it, as to KeyPoint, anything?

One of the things that is so interesting from our perspective of -- we're lumped in with OPM here, the real key of their allegation on traceability or causation is in paragraph 127, where they talk about, essentially -- and I'll quote from it, Your Honor, because I think it is naked in its detail and because it is not clothed, therefore, it can't go forward.

And it says on May the 7th of 2014 hackers accessed OPM's network using stolen KeyPoint credentials. It at no point --

THE COURT: It has the passive voices running all through there. It doesn't --

MR. WARIN: It doesn't say. Your Honor, it doesn't say how, when, by KeyPoint? When? And then if you juxtapose that to the 38 plaintiffs and you say, well, when did you fill this form out? One of the things plaintiffs counsel said, well, when we interviewed people, they felt this or they believed that. But the complaint does not -- and if you go through every plaintiff, it doesn't say on 1-1-2009, I, F. Joseph Warin, filled out an SF-86, it contained this data, and then proximate in time that data was used and injured me in fact.

THE COURT: Well, and that, I think, we've gone over. And certainly I've read all those allegations and I

understand that. So I don't want to cut you off because I know you have a lot of good things to say, but I want to focus on the things that we haven't focused on yet.

MR. WARIN: Sure. And Mr. Mendro with argue the immunity, contractor immunity in just a moment, Your Honor. But I would invite the Court's attention to your colleague's decision in *SAIC* that does talk about the issue that was raised there. And I think it, frankly, is contrary to plaintiffs' counsel's statement.

It says: There is, no doubt, cold comfort for the millions of servicemen and -women who must await and watch their credit reports until something untoward occurs. After all, it is reasonable to fear the worst in the wake of such a theft. It is understandable, frustrating to know the safety of your most personal information could be at danger.

The Supreme Court, however, has held objective reasonable likelihood of harm is not enough to create standing. And even if -- not enough to engender some anxiety, he goes on to say. And *Spokeo* comes behind that, Your Honor, and so it only acts as a buttress for that argument, to be able to say, well, you need more of that, as the Supreme Court -- it's ironic, I'm old enough to remember when *Blacks Law Dictionary* was cited often. But it was interesting in *Spokeo*, when they're talking about injury, what type of injury they're talking about. They're talking

about de facto injury, citing *Blacks Law Dictionary*. And that's because that's the nature of the injury they're required to have.

THE COURT: Well, I think you could put, you know, 20 philosophers in a room and they could be there for months debating the question of whether the theft of data is abstract or concrete.

MR. WARIN: I agree.

THE COURT: But I don't know that we have to go there because there's all these other requirements. It has to be concrete in the way it's been defined by the Supreme Court, and imminent.

MR. WARIN: And particularized.

THE COURT: Right.

MR. WARIN: Right. And so if you -- and then when you get to --

THE COURT: Well, particularized I think they've got. They know it's them. The government sent them a letter and said it's you. And I think the particularized requirement is usually to distinguish the people who just don't like the federal government's policy on whatever, but there's no indication that it touches them. I'm not sure that I'm going to -- this is going to lose on particularized because the first letter was May, maybe your data was taken, but the second letter said you're in the breach, it's you.

MR. WARIN: One of the things, the Court gave the plaintiffs an opportunity -- so, notified in May, notified in June, first complaint filed in June, amended complaint filed in March of '16. We hear from plaintiffs' counsel that they interviewed people. At no point do they do the traceability or the causation to our client, KeyPoint. No one says I gave this data to KeyPoint or KeyPoint was the semiquinone of this circumstance. But they just throw, in paragraph 127 and paragraph 7, data breaches and so forth. And as we can see, there's a continuing data breach allegation in the complaint, and I think the Court can rely upon that. And so it only heightens the requirement of plaintiffs in this as it relates to the defendant.

We fundamentally disagree that -- with the plaintiffs' counsel's statement that it doesn't have to be a claim-by-claim, defendant-by-defendant analysis; it clearly does. The *Daimler* case, which our firm handled at the Supreme Court, absolutely commands it is a claim-by-claim analysis. *Spokeo* certainly has that. And then the question becomes, as one looks at traceability, is this something that takes it from the possible to the plausible? And, you know, or as stated in *Twombly*, from the conceivable to the plausible. And if you look at those themes, it echoes off this complaint. There's nothing here as it relates to KeyPoint.

And lastly, Your Honor, I would say the elephant in the room that the Court asked about, we do think that you can take into account that this was a state sponsored attack. And because it does tease out the things that come out of the Seventh Circuit --

THE COURT: What do I cite for that proposition? You know, I was trying to find out if anyone in the federal government has said so. And according to Congress, the *Congressional Report* only talks about the former head of National Security. Newspaper accounts talk about the current. You know, I have, as a practitioner, disdained District Court Judges who cited the *New York Times* for some proposition, other than the fact that this is in the *New York Times*. I mean, for the fact, what do I cite for the fact?

MR. WARIN: Well, certainly the House, House committee report of early September is something you can cite for that fact. And it gets you --

THE COURT: It quotes -- the Hayden quote on page iii, before you even get -- in the actual report it doesn't talk about it because, I guess, it was congressmen who received that information in classified briefing and they may have come outside and made a statement, but they didn't put it in there.

MR. WARIN: Right. And I understand that the

government is in a different posture than KeyPoint is. But from KeyPoint's perspective the Court can rely upon that and it's really part of that whole --

THE COURT: I invite you, if you would like to find some document or someone with some official status said it out loud or something besides, you know, what I came up with in ten minutes, you're happy -- I'm happy to receive it because I think it relates to the targeted nature of the breach, it relates to the nature of the harm, it relates to causation, it relates to everything and no one is talking about it.

MR. WARIN: Right. And that's why I call it the elephant in the room, Your Honor. Because unlike in *Neiman Marcus* where you have 350,000 intrusions of credit card, debit, and then 9200 of them used, so the linkage is completely drawn between the incursion and the harm. Here, this is a scattershot of harm unrelated in time, unrelated in location, unrelated in approach. It's a grab bag of utility bill and a tax refund and a discount and so forth.

Thank you, Your Honor. I'm going to let my colleague Jason Mendro put the icing on the cake.

THE COURT: Seriously, if there's something that you can file, a supplement that just points me to something that describes the source and nature of this breach, I think it bears directly to the arguments they're asking me to look

at, which is the targeted nature of the breach and the purpose of the breach and the risk of the breach and whether that risk is reasonable. So, if you would like to give me something that the government won't give me, go right ahead.

MR. WARIN: Thank you, Your Honor.

THE COURT: All right.

MR. MENDRO: Good morning, Your Honor.

THE COURT: Good morning.

MR. MENDRO: Jason Mendro for KeyPoint. KeyPoint is in this suit for one reason and one reason only. It's because KeyPoint was standing in the shoes of the federal government in conducting background checks on applicants for federal jobs.

It has been settled Supreme Court law now for more than 75 years that a contractor performing the work of the government, as the government directs, is entitled to immunity. That's the rule that was set down in 1940 in the *Yearsley* case. It's been reaffirmed time and again, and reaffirmed most recently just this year in *Campbell-Ewald versus Gomez*, where the Court said, quote, Where the government's authority to carry out the project was validly conferred, there is no liability on the part of the contractor who simply performed as the government directed.

That rule compels dismissal of all of the claims against KeyPoint, Your Honor. The complaint pleads

repeatedly, beginning in its very first sentence, that KeyPoint is a government contractor. It pleads that KeyPoint performed its work pursuant to a contract with OPM. It is undisputed that OPM had the authority to enter into that contract and it is undisputed that that contract is valid.

THE COURT: All right. Well, let me stop you here. And that's a very helpful statement of the law, but I did actually read what you wrote. And so my question is: Where does negligence fit into this analysis? Do you agree -- I understand that failure to comply with the government's directives, unauthorized -- acts that weren't authorized under the contract could fall outside the scope of the immunity, but what about negligence?

MR. MENDRO: So the plaintiffs raise only three arguments in response to immunity, and one of them is the negligence argument. All of their arguments are overlapping and basically boil down to contention that immunity can be made to go away simply by using magic words, that all the plaintiffs need to say is that the immune contractor was negligent or not reasonable and immunity simply doesn't apply. That's not the law, Your Honor. The word "unreasonable" appears in the Fourth Amendment.

THE COURT: I want to specifically talk about negligence because it isn't one of the exceptions set out in

the most recent case. There are a couple -- there's a case; from 1943 where they mention it, then in 1949 they say, Well, that doesn't necessarily make sovereign immunity go away, the *Larson* case. But, then the term pops up here and there. Judge Walton mentioned it in the *Fort Totten* case, which was a case where it was the sovereign that was suing -- doing a cross-claim against the contractor.

But I just want to know, what's the status of that legal principle? Can negligence vitiate the immunity, or not? And then, if so, isn't that a question of fact? So how would you dismiss the allegations as a matter of law?

MR. MENDRO: The answer, Your Honor, is that immunity cannot be vitiated unless the plaintiffs plead a violation of clearly established law. They may be able to plead that an act was negligent if they can plead that it's clearly established that that act was negligent. But they can't simply assert the word immunity -- or, the word negligence, ratter, and overcome immunity.

As you noted, immunity was not -- or, negligence was not mentioned in *Yearsley*, it was not mentioned in *Campbell-Ewald*. I think the 1943 case the Court is referring to is probably the *Brady* case, which is strictly limited to the suit in Admiralty Act and is not applicable here.

So there are no cases that say that simply

asserting negligence overcomes immunity in all instances. That's the magic words test that the plaintiffs would like the Court to adopt. And I submit that would be an erroneous decision.

You mentioned Judge Walton's decision in *Fort Totten Metro Rail* and that case is distinguishable because the contractor in that case was in clear violation of the government's contract. That's one way in which immunity might --

THE COURT: He said they were negligent. He cites the principle, he said negligence can take you out of it. And he points to -- I think it's *Ackerman* and *Brady*, but then he says here WMATA says they were negligent and, and so --

MR. MENDRO: That's precisely right, Your Honor. The contractor in that case was hired to install devices on railroad tracks that had to be compatible with other devices that were already installed. That was a crucially material term of that contract. And the failure to comply with it resulted in a fatal train accident. The contractor didn't install compatible equipment, didn't safety test the equipment as it had promised in its contract for compatibility. And for that reason the government was actually suing the contractor. There is no dispute that that contractor was not carrying out the role of the

sovereign. That contractor was in litigation with the sovereign.

And this case is nothing like that. I'm sitting at the same table today as the Department of Justice because we are alined in seeking dismissal of these claims. The plaintiffs plead that OPM never fired KeyPoint after these events. The plaintiffs specifically plead that KeyPoint's access was never taken away to OPM files. They specifically plead that KeyPoint was never suspended, yet at the same time the complaint pleads overtly that another contractor was terminated.

So there's nothing in the allegations that suggests that KeyPoint was not carrying out the role of the sovereign, and there was nothing other than pure say-so to suggest that KeyPoint was in violation of the government contract. The only thing that the plaintiffs assert about the contract is that it incorporates the terms of the Privacy Act. But there's no allegation of any requirement that was in the contract that KeyPoint didn't comply with. And the assertions about the Privacy Act are nothing more than threadbare assertions of a violation.

There's no allegation that it was ever clearly established that KeyPoint was required to do any particular thing under the Privacy Act, nor is there any allegation that that thing wasn't done. And that is precisely the sort

of allegation that the Supreme Court rejected in *Ashcroft versus Iqbal*, the very case that teaches us what it means to plead an insufficient claim --

THE COURT: When they specifically say the contract incorporated the Privacy Act, that -- they don't actually attach the contract, but you don't come back and say that's not true, and I have to accept their representations as true. So that's a fact as far as this motion is concerned, that it does do that.

MR. MENDRO: We don't have to dispute the contract incorporates the Privacy Act because the allegations about the Privacy Act are completely insufficient. If the Court looks to paragraph 123 of the complaint, which is the paragraph that the plaintiffs appear to rely on most in their brief for their immunity argument --

THE COURT: They say you violated the Privacy Act.

MR. MENDRO: That's exactly right, Your Honor. That paragraph is a textbook legal conclusion. You can compare the language in paragraph 123 and you will see that it quotes almost verbatim the language from the Privacy Act and concludes with the barest assertion that KeyPoint was in violation.

THE COURT: Well, and if the Privacy Act doesn't impose any obligations on private parties, one could argue that a contractor can't violate the Privacy Act. But you've

also said we are standing in the shoes of the government here. So, can you violate the Privacy Act?

MR. MENDRO: We cannot violate the Privacy Act, with one exception. There is a provision of the Privacy Act that says that we will be treated as employees for purposes of criminal liability. I believe that is Title 5 U.S. Code section 552a(m). But, beyond that, it is true that contractors cannot violate the Privacy Act. They are answerable to the government for the performance of their work.

But that's neither here nor there, Your Honor, for the simple reason that there is no well-pled allegation of a violation of the Privacy Act in any event. It's simply a threadbare assertion of the type that was rejected in *Iqbal*. In *Iqbal*, the very case that teaches us what it means to plead an insufficient claim, was in fact a qualified immunity case, dealing with the very same issues that we're dealing with on the pleadings at this stage of the case.

This Court has done the same in --

THE COURT: You don't have to tell me cases where I've cited *Iqbal*, for goodness sake. I do that every day.

All right. So I don't think I have any more questions for you. If there's any other points you want to make that you think I need to hear, I'll let you make them.

MR. MENDRO: The only other point I would make,

Your Honor, is the policy point, that our government depends on contractors to do its important work and has since the beginning of the republic. In *Filarsky* a unanimous and scholarly decision by the Chief Justice, he said that uncertain immunity is little better than no immunity at all. And without immunity that actually counts, that can be relied upon, the government is not going to be able to rely on contractors, or otherwise have to indemnify them at tremendous cost against claims that the government itself can never face.

And that is unreasonable as a matter of policy. It's inconsistent with seven decades of Supreme Court law and it would be disastrous for taxpayers.

THE COURT: Thank you.

All right. Who on the plaintiffs side is doing this issue? Okay.

MR. PATTERSON: Thank you, Your Honor. I'll turn to the contractor immunity. One thing on the standing, with respect to whether some *Congressional Report* comes in or something like that, we obviously would want an opportunity to respond to anything that KeyPoint would put in on that.

THE COURT: Well, the only thing I'm asking them to do is to provide me with citations to anything that's public and official that says this was a state-sponsored breach and we're specifically -- it emanated from China.

Now, if there's something after you see that that you want to bring to my attention, you're welcome to do that. But I'm not asking for a brief about the impact of whether it's state sponsored or not on these issues.

MR. PATTERSON: Right. Well, and our understanding is that you can take notice that those people said that, but you cannot take notice that it's actually true. So it wouldn't -- it wouldn't advance the ball in terms of what can be accepted for purposes of the motion to dismiss because as the government said --

THE COURT: In the end it's what have you alleged.

MR. PATTERSON: Right. Exactly.

THE COURT: And certainly you haven't alleged that the purpose of this was to get people's Social Security information or credit card information so that it could be used to anyone's financial advantage. You haven't alleged a purpose at all, so --

MR. PATTERSON: We've alleged that it was malicious and we've alleged that these events followed involving Social Security fraud, so a plausible inference from that is that's the purpose. Another inference is there could be another purpose. But on the motion to dismiss the inference --

THE COURT: Did they use word the "malicious"? That's enough.

MR. PATTERSON: I'm saying the facts taken as a whole, a malicious attack that exfiltrated this specific information that has then resulted in plaintiffs experiencing specific harm using that information --

THE COURT: Well, you didn't even say that. All you said is this happened and then this happened. You're asking me to conclude that it's as a result of, but I don't think that you argued it, other than in your first general paragraph. But, we've talked about standing.

MR. PATTERSON: Right. So I just wanted to make that one point about --

THE COURT: Let's go right into malicious. In paragraph 123 you say KeyPoint violated federal law, in particular the Privacy Act.

MR. PATTERSON: Yes.

THE COURT: Now, the Privacy Act doesn't impose violations on private parties and doesn't permit suits against private parties. You also alleged in paragraph 114 that there was an intrusion on KeyPoint that was sophisticated and malicious. That's where you use the word "sophisticated and malicious." So is it a violation of federal law to be a victim of a sophisticated and malicious attack?

MR. PATTERSON: It's a violation not to take reasonable precautions when you know that this information

is very valuable and it's subject --

THE COURT: Where do you allege in the complaint that KeyPoint violated federal law by failing to take reasonable precautions to prevent the December 2013 intrusion?

MR. PATTERSON: We allege in the -- well, we allege in the negligence count all the things that were insufficient with KeyPoint system, which as my colleague mentioned, I believe begins in paragraph 217, or around there.

But the Privacy Act does apply to contractors. 552a(m) specifically says that when an agency provides, by a contract, for the operation by or on behalf of the agency of the system of records to accomplish an agency function, the agency shall cause the requirements of this section to be applied to such system. So the requirements of the Privacy Act by federal law apply to KeyPoint.

THE COURT: Well, you said they violated federal law, which is a legal conclusion. What are the facts that support the legal conclusion? The negligence?

MR. PATTERSON: Yes. So, 552a(e) requires entities subject to the Privacy Act to have appropriate safeguards on the information that's in their control. And our -- the whole thrust of the negligence count and the other counts detailing the KeyPoint breaches is that they did not have adequate safeguards protecting their information.

THE COURT: You say that the contractor is not immune if it violates the term of the contract. Is the only specific contractural term that you allege was violated is the term that imports the Privacy Act?

MR. PATTERSON: Yes. That's the only specific term that we allege that was violated.

THE COURT: All right.

MR. PATTERSON: But to back up a little bit --

THE COURT: But when you say they breached the contract and they breached the statute, isn't that very conclusory when you also say, in paragraph 5, as soon as OPM knew about the KeyPoint breach it didn't take any action against KeyPoint, it didn't suspend the contract or invoke any remedies. So what facts in the complaint plausibly allege that the contract was violated?

MR. PATTERSON: Well, we don't know what went on between -- we know they didn't take KeyPoint off the contract, but --

THE COURT: You allege that.

MR. PATTERSON: We know that, but we don't know why. We don't know what happened between the government and KeyPoint. I mean, at this point on a motion to dismiss, you know, it doesn't make sense to say that we have an obligation to say that -- why the government did not pursue contract remedies against KeyPoint.

THE COURT: You have an obligation to set forth facts and not legal conclusions. You specifically argue in your motion that the contractor violated the terms of the contract and it failed to follow OPM's directives. And I'm asking you to point me to one fact that you've alleged that supports either one of those conclusions.

MR. PATTERSON: Well, the facts that we have alleged are the facts relating, as I said, to the Privacy Act violation by not having adequate safeguards on the system, that was one violation. The other violation was the unlawful disclosure of the information. And those acts -- you know, whether the federal government, you know, sought to enforce it or not in terms of its contract, the federal law requires KeyPoint to follow the requirements of the Privacy Act.

But the Privacy Act is only one of three independent reasons, the breach of contract, why contractor immunity does not apply here. I mean, the first reason is that, as the Supreme Court has said in *Correctional Services Corporation*, summing up contractor immunity, that's 534 U.S. 61, it says, Contractor immunity applies where the government has directed a contractor to do the very thing that is the subject of the claim.

So the only time --

THE COURT: They've directed them to collect this

information.

MR. PATTERSON: Right. But that's not specific enough. If you read the *Boyle* case, which extended contractor immunity to procurement contracts, Justice Scalia specifically said if it is possible for the contractor to comply with the contract and its state law of duties, then immunity does not apply.

So, you know, KeyPoint is not up here saying it would not have been possible for us to protect this information in ways that the plaintiffs say we should have because the government said we couldn't, they're just saying we are a contractor --

THE COURT: I don't see how your claim arises out of anything other than what they were doing under the contract.

MR. PATTERSON: Right. It's what they were doing under the contract, but it wasn't things that they were specifically directed to do. At least we have not alleged that the government specifically directed them to have inadequate safeguards and to not train their employees.

THE COURT: You said they were specifically directed to comply with the Privacy Act and they failed. So you're talking about what is specifically directed under the contract, aren't you? You're not saying they also went out and provided, you know, transportation services and that wasn't under the contract, so if they did that negligently --

MR. PATTERSON: No, but we're saying that it would have been possible for them to protect our information adequately and also to follow the government's directives. And in *Boyle* it says there's no immunity in that situation, it's only -- and in *Boyle*, for example, the government specifically ordered helicopters -- they specified the design. They said it has to open outward. And then the plaintiff said, well, that was a faulty design because because it opened outward when it crashed in the ocean, our pilot couldn't get out because of the water pressure. But the Court said there's immunity there because the government specifically told you to put that feature in the helicopter so you're immune.

But Chief Justice Scalia -- or, Justice Scalia also specifically said that there would have been no immunity if the government had just ordered a stock helicopter and it happened to open the wrong way.

So if it was possible to comply with both the government contract and the state law of duties, then there's no immunity.

THE COURT: I'm not sure that case goes that far and I'm not sure that that's what you were saying in your opposition. I thought you said the reasons it wasn't immune is because they violated the law, they were negligent, and they violated the terms of their contract and failed to

follow OPM's directives.

MR. PATTERSON: Well, in terms of directives, we would say there were no relevant directives, at least that we're aware of, that would have prevented OPM -- or, KeyPoint from protecting our information. So, it wasn't -- when it failed to protect our information, it wasn't following the government's directives.

And the other reason, and you touched on it with counsel for KeyPoint, is negligence.

THE COURT: But all you're saying is -- it seems to me very, very circular, that if we allege that something went wrong in terms of your performance of your contract, we have alleged action outside of the contract and that means that the hole that you just described in immunity would be a hole in every case.

MR. PATTERSON: It's not a hole in every case because it wasn't a hole in *Yearsley* because there what the plaintiffs were attacking was this project that caused erosion on their land. And the Court said that was an inevitable consequence of what the government ordered. The same thing in the *Ackerson* case from the Fifth Circuit involving the Mississippi River gulf outlet that they cite.

The Court made very clear the plaintiffs were attacking the negligence of the whole project, the harm that inevitably resulted from the project. The same thing from

the *Butters* case that they cite which involved foreign sovereign immunity and discrimination. And the Court specifically said, well, there's immunity here because Saudi Arabia ordered the discrimination. If the contractor had done the discrimination themselves, there would be no immunity.

So it's very clear running through all these cases, the *Boyle* case I already mentioned with the helicopter, it's very clear running through all these cases, it's only when the decision that's being attacked is the government's decision that immunity applies. The immunity --

THE COURT: Well, you're not talking about the decision, you're talking about --

MR. PATTERSON: Or the actions.

THE COURT: -- care in implementing the government contract, of performing their duties under the contract.

MR. PATTERSON: Right. So -- and another case that I can cite you to that I believe was not -- I don't have it here, but the D.C. Circuit case involving torture of prisoners at Abu Ghraib said that the contractors were immune because they were under the direction of the military chain of command. But they said if it had been an order of work that just said accomplish this result or do this thing, under -- you know, and you implement it, there would have been no immunity.

So, it's clear from these decisions that it's -- the reason the contractor gets immunity is because if -- if the plaintiff is really attacking a government decision or government action, something that the government itself is responsible for. Here we are saying there are independent things that KeyPoint did wrong that it is responsible for, and that is why they're not immune. And related to --

THE COURT: Is that inconsistent with your argument that the contract specifically incorporated the Privacy Act? You're saying on the one hand they violated federal law because the contract specifically directed them to handle information in a particular way, and now you're saying that the particular way which they handled the information is not what they were directed to do by the government, so we get to sue them for that.

MR. PATTERSON: Well, first, we're saying they didn't handle it consistent with the Privacy Act. But second, let's say they did abide by the Privacy Act, which we, again, don't accept, but they still -- that would not have prevented them from doing other things that would have protected our information that we say fell short. And again, in the *Boyle* case, it very clearly says if it's possible --

THE COURT: So they should have done more than the government told them to do in terms of protecting --

MR. PATTERSON: Yes. And the *Boyle* case makes clear, it's really a preemption question.

THE COURT: Why do you get to decide that, if they're supposed to do what the government asks them to do?

MR. PATTERSON: Because they still have a duty to people outside of the government, even when they're a government contractor. And that is from the *Brady* case that you discussed. I think that's clear from the -- involving the negligence from the U.S. Supreme Court, and also from the *Boyle* case. Again, it's really a preemption question. Is there a conflict between the contractor doing what state law would require them to do and doing what the government is telling them to do? If they can consistently do both things, there's no immunity.

THE COURT: Well, what's their state law obligation here?

MR. PATTERSON: Well, here we've raised several claims; negligence, invasion of privacy, there are consumer fraud type of statutes, contracts. We've got several claims that we've alleged against KeyPoint and those go to the merits of whether -- they have arguments on the merits, but it's not before the Court today.

You also ask about negligence. I mean, the *Fort Totten* case clearly --

THE COURT: When you alleged in paragraph 121 that

we don't even know how the breach happened at KeyPoint --

MR. PATTERSON: Right.

THE COURT: -- how does the complaint plausibly support the allegation that the contractor was negligent and that's how the information got out the door?

MR. PATTERSON: Well, we say that they lacked the software to track their systems and that this person, or whoever it was, was in their system from December to September without anybody even knowing it. So that had they adequately secured their systems and not let the person get in in the first place, and then adequately monitored the system to figure out that the hacker was in there, then the harms would not have happened.

And similarly, with the stolen credential, if that credential had not been stolen, it, you know, possibly could have eliminated the entire breach at OPM because that's what was used to hack into OPM's systems.

THE COURT: Is there anybody who's been told that their data was stolen in the OPM data breach that we know that their data was stolen in the KeyPoint data breach?

You're saying there was a hacker in KeyPoint and they didn't do enough to find him.

MR. PATTERSON: Um-hum.

THE COURT: Period. And then you say KeyPoint login credentials were what got to the OPM data breach and

it was the OPM data breach that told all these people your data is missing. So from that first thing, the hacker who was hacking around in KeyPoint, you're not alleging that any of your plaintiffs, their data walked out the door as a result of that?

MR. PATTERSON: Let me check with my --

MR. GIRARD: No.

MR. PATTERSON: No.

THE COURT: Okay. So that happened. That's a bad thing, but that doesn't have anything to do with any of the allegations in the complaint.

MR. PATTERSON: Well, it reinforces their negligence in managing their systems and makes those allegations plausible.

THE COURT: That doesn't make them negligent to you, that makes them negligent to the government because you haven't said that that's why your data went out the door.

MR. PATTERSON: Correct.

THE COURT: Okay. So now we've got keeps stolen KeyPoint login credentials opens the door at OPM. And what does that have to do with all these inadequate things that you said they did?

MR. PATTERSON: Well, we've said that they -- well, first of all, we don't allege in the complaint, and I don't know if we know how the person got those credentials,

whether it was through the data breach or through physically getting to someone at KeyPoint. And we've said that they inadequately monitored and trained their employees, including when their workforce went up due to increased workload with the federal government, that they didn't hire more supervisory employees. And we've also said that they haven't -- that they did not secure their system. So how ever that --

THE COURT: Stolen login credentials.

MR. PATTERSON: Right. Stolen, yes.

THE COURT: Okay. So, I mean, I guess this goes back more than to immunity, to the first KeyPoint argument, which is you got all this harm that happened to all these people and then you have these inadequacies over at KeyPoint, and you haven't connected them in any way.

MR. PATTERSON: Well, we've connected them in saying that they were inadequate in securing the login credentials of their employees and those credentials are what was used to perpetuate the OPM breach.

THE COURT: And where is the specific paragraph where you say they were inadequate in securing login credentials?

MR. PATTERSON: Let me see. So, paragraph 228 specifically says plaintiffs and class members sustained harm as a result of KeyPoint's negligence in failing to

protect and secure its user login credentials.

THE COURT: Right. But that's a conclusion. Where is there any indication -- where do you allege just, first of all, that they were negligent in failing to secure their login credentials?

MR. PATTERSON: Well, I think it's in the negligence count, and then also paragraph 122 says by unreasonably failing to safeguard its security credentials and plaintiffs and class members' GII, KeyPoint departed from its mandate, exceeded its authority and breached its contract with OPM.

THE COURT: All right. Okay. Anything more that you want to say about government contractor immunity?

MR. PATTERSON: Just briefly. They asserted we had to show clearly established -- some clearly established violation. There's no case holding that. In certain circumstances, in 1983 cases, which is the *Filarsky* case that they mentioned, contractors have gotten qualified immunity. But, you know, this isn't a 1983 case. This is not against an individual, it's against a corporation. And there's also is a case called *Richardson*, which *Filarsky* cites, 521 U.S. 399, where it was an employee of a corporation that was operating for profit and that it had taken on administration of a prison. And the Court said in that circumstance where it's a long-range thing, it's a

corporation, there are market pressures, there's no qualified immunity. And we submit that same argument would apply here.

THE COURT: Okay. All right. Thank you.

Let me hear briefly from the contractor immunity lawyer on the -- I'm sorry, I forgot your name, Mr. Mendro -- on this issue.

Basically can you address the one thing that you didn't talk about, which is his argument that since what they're talking about is a duty that's separate from the contract duty, not even consistent with the contract duty, that it doesn't fall under the contractor immunity.

MR. MENDRO: Yes, Your Honor, gladly. The answer to that question is the clearly established requirement. The plaintiffs assert that we have to comply with state law as well as federal law, and I don't think there's any dispute about that. But we're immune from both unless the plaintiffs can plead that there's a violation of clearly established law. That's not an impossible thing to do.

Clearly established requirements can come from statutes, they can come from regulations, they can come from cases. And *Campbell-Ewald* is a very good illustration for that. I was a little surprised to hear plaintiffs' counsel say that there are no cases that discuss the clearly established requirement in this context because

Campbell-Ewald did exactly that thing.

In the majority opinion authored by Justice Ginsburg, she analyzed both *Yearsley* and she analyzed the *Filarsky* requirement, the clearly established requirement. She applied fact to law. It was material to her holding. And I don't think that it's reasonable to infer that the Supreme Court would have had that discussion if that law did not apply to contractors.

I would also note that *Campbell-Ewald* is not a 1983 case. It's true that the clearly established requirement has been applied extensively in lawsuits against police officers and other officials who are being sued under 1983, but *Campbell-Ewald* was a lawsuit under the Telephone Consumer Protection Act and the same analysis was applied in that case.

I was grateful that plaintiffs' counsel mentioned the *Ackerson* case in the Fifth Circuit because that case is exactly like this case. And I would urge the Court to consider it.

THE COURT: I've looked at it and I think it sort of takes the question of negligence -- it doesn't hold that an allegation of negligence saves the complaint later. It's been held that it doesn't hold that, it just noted that the people hadn't alleged negligence.

MR. MENDRO: But what I do think is informative

about the case, Your Honor, is that it's directly contrary to the argument you heard that it's only the government's decisions that are protected by immunity. That, too, was a negligence case. It was a negligence case against a contractor who's performing dredging work. And the Fifth Circuit rejected allegations exactly like this one, saying that they were only conclusory. And when the plaintiffs came back and said we would like to add some allegations about violations of various laws and regulations, the Fifth Circuit considered those and said it would be futile to add those because you're just making conclusionary assertions, and conclusory assertions just don't cut it to overcome immunity.

THE COURT: All right. Thank you.

I wanted to ask Mr. Warin one more question about causation. I recognize we've got all the issues about imminence and actual harm, but if they say in their complaint they didn't protect their login credentials properly, their login credentials were stolen, their login credentials are the keys to the kingdom at OPM, is that sufficient just for standing purposes to allege that there's some connection between what they say you did wrong and what they say happened?

MR. WARIN: No. And it's because, you know, two coincidences need to be bound together for there to be

traceability, and causation needs to say this happened because of A, B, C. You can't just say, well, there was genesis and then all of a sudden we get to the kingdom. You need to say on the first day X happened, on the second day X happened, on the third day X happened. There needs to be a linkage there. That's why, Your Honor, I pointed out --

THE COURT: Well, if somebody came in your house and put your television and your stereo and your computer and all your appliances out on the front porch and then somebody walked by and stole it, isn't that a reasonably foreseeable consequence of the person who put it on the front porch?

MR. WARIN: But there's nothing in the complaint that says that we put the things on the front porch. What it --

THE COURT: I think they're saying, in the negligence section, that you didn't do what you needed to do to protect --

MR. WARIN: But the negligence claims, when you look at them, essentially they're circular. They essentially just parrot what a negligence claim would be, as opposed to articulate facts that are particularized and clear that's linkage. So that's why paragraph 127 is so vital to us in the argument, because of the way it is articulated. And one of the things, when you piece through

paragraphs 13 through 50, which are the plaintiffs claims, you know, when you look to say what -- link up for me, would you, please, Jane Doe with the SF-86 and KeyPoint, there's not an iota of linkage. And because of that, both on standing grounds and, obviously, on traceability grounds, their complaint falls.

THE COURT: All right. Thank you.

MR. WARIN: Thank you, Your Honor.

THE COURT: All right. I know that I said one of the things I would also take up today was the motion to dismiss the NTEU complaint on standing grounds. I think that everything that has been discussed here relates specifically to that. Is there anything that is not repetitive that you want to say about standing in your complaint that hasn't already been said by this team here that has been arguing standing for two and a half hours?

MR. SHAH: Yes, Your Honor.

THE COURT: All right.

MR. SHAH: Your Honor, I would like to focus on two things. The first is our primary argument for standing, which is set forth in pages 8 through 11 of our opposition. OPM did not respond to that argument in its motions papers. And that's our lead argument and we would like to flesh that out for the Court today. We would also like to focus on OPM's *Lyons* argument, which is its primary argument in this

motion.

THE COURT: Its what?

MR. SHAH: Its primary argument in its motion to dismiss.

THE COURT: Its what argument?

MR. SHAH: Primary.

THE COURT: No, the one before that. You said we wanted to focus on their something argument, which is their --

MR. SHAH: Oh, sorry, Your Honor. Their *Lyons* argument.

THE COURT: *Lyons*. Thank you.

MR. SHAH: Yes. Your Honor, our primary theory of standing is tied directly to our basic legal claim which must be assumed to be valid for purposes of this standing inquiry. And that basic legal theory is this: That where inherently personal information, information like Social Security numbers, financial information, medical information, information about one's spouse or partner that is personal, when that type of inherently personal information is provided to the government on an explicit promise of confidentiality, where the government disregards that promise, the constitutional right to informational privacy is violated.

Here we allege that constitutional violation occurred and that we, therefore, suffered an Article III

injury the moment that hackers took our members' inherently personal information from databases that OPM recklessly refused to secure for nearly a decade, despite the urgent warnings of the inspector general.

THE COURT: All right. But if I have to do standing before I do 12(b)(6), then is there really anything different between your argument and the other plaintiffs' argument that the injury is the departure of the information? You're saying it's a constitutional injury, they're saying it's a common law injury. But you're both saying that's the injury, nothing more is needed.

MR. SHAH: Your Honor, there is a difference. And the difference is illustrated in the Second Circuit decision, *ACLU v. Clapper*, which is discussed in our opposition. There the Second Circuit does two things that are pertinent here. First, it accepted plaintiffs' legal claim as valid for purposes of the standing inquiry. And second, it views standing through the prism of the particular claims raised.

In a *ACLU v. Clapper*, plaintiffs there raised First and Fourth Amendment claims related to the government's collection of metadata from their private phone communications. Accepting the plaintiff's legal theory as a valid one, the Second Circuit said this, they said that where the allegedly unconstitutional act was the collection

of the metadata itself, then and there plaintiffs suffered a cognizable, Article III injury.

THE COURT: But there the question of whether the collection of data relates to the constitution, it seems to me, is a little more clear. So here don't I have to sort of tread a little bit down the merits road to answer your question? What if I don't think there is a constitutional right to data protection?

MR. SHAH: So, two things there, Your Honor. We do believe that for purposes of the standing inquiry you must accept our legal theory as a valid one, unless it is, in your view, entirely frivolous, which we don't think our theory is.

Second, Your Honor would be on firm ground assuming and concluding that the constitutional right to informational privacy exists and that it continues to persist even after information has been disclosed to the government. The government, in the post-disclosure context, continues to have a duty to safeguard the information that it collected on the promise of confidentiality.

And that's really our legal theory here, and it is buttressed by decisions in five different courts of appeal where Courts have evaluated claims in the post-disclosure context. Those cases -- and those are decisions by the Fifth, Eighth, Ninth, Tenth, and Eleventh Circuits. Those

Courts have concluded that where the government takes the information on the promise that it will protect that information and keep it confidential, that promise can't be a hollow one. It then must follow through and it can't, for example, take that information and disclose it to a third party. Here we're in an area where --

THE COURT: But the obligation to protect it against sophisticated and malicious theft, that's constitutional or that's statutory?

MR. SHAH: Your Honor, we believe it's constitutional. We believe the government has a constitutional obligation to protect the inherently personal information that it took from our members on the promise of confidentiality, which our members had to provide to it as a basic condition of their employment.

THE COURT: Is it the fact that it's missing that makes it a constitutional violation or the fact that they didn't secure it sufficiently?

MR. SHAH: The latter. Their reckless indifference in securing the information, which we believe led to the breaches that occurred in 2014 upon the taking of that information by the hackers who did not have the authority to view or have that information. That was the allegedly unconstitutional act.

THE COURT: Well, aren't there some cases that say

that sometimes the standing inquiry and the merits inquiry are mixed and you have to get into it a little bit? It seems to me that you are relying heavily on your merits argument to create standing. So don't I have to look at them together, if you're saying I have standing for a different reason than everybody else?

MR. SHAH: Yes. And we think that would be appropriate here. We think the Supreme Court's decision in *Warth v. Seldin* certainly indicates that the nature and source of the claim asserted is relevant to the standing inquiry. And that's really a core basis of our standing argument here. We think if you look at *Warth*, which says take the claim into account, and if you look at *ACLU v. Clapper*, which truly did involve First and Fourth Amendment claims, but at their core those are individual constitutional privacy rights, like ours. And there the Second Circuit said that where you allege that the constitutional violation occurred, that is your Article III injury, that allegedly improper and unconstitutional act. And so here, for us, that would be the taking of the information from the databases that OPM recklessly failed to secure for over a decade.

THE COURT: All right. And why don't you address the *Lyons* issue quickly and then I think we'll probably wrap up for today.

MR. SHAH: Certainly. Certainly. We certainly agree, Your Honor, that under *Lyons* we must credibly allege a realistic threat that our alleged injury will reoccur, given the prospective relief that we seek. And we believe that we've done that here.

The real question for the Court here is have we credibly alleged, within reason, that valuable targets here, databases containing inherently personal information for millions of federal employees, including our members, have we credibly alleged that those valuable targets will be targeted for a third time? And we believe the answer is yes.

Looking at our complaint, in particular paragraphs 87 through 91, we note that OPM's inspector general continues to have real concerns that its data base are properly secured. In November 2015 OPM's then inspector general said he's, quote, very concern the agency's systems will not be protected against another attack. Around that same time period, looking at the agency's plans to revamp its information security, the inspector general says, quote, there's a high risk that OPM's project will fail.

And even more recently, just months ago, in May 2016, and now looking at OPM's current plans to revamp its IT infrastructure and security, the I.G. said he's, quote, even more concerned. In other words, more concerned than ever the project will fail. These systems are ripe for

attack, they're still vulnerable for attack.

THE COURT: There's a risk, you're saying, of the same harm, which is just the private information walking out the door. But you're not arguing that -- and that your constitutional harm will flow, but not a risk of financial harm, that kind of thing?

MR. SHAH: So, Your Honor, we allege that there's a realistic threat of another breach of OPM's still deficiently secured data systems that would expose our members' inherently personal information, which we allege is an Article III injury.

We do have an additional standing theory that begins on either page 11 or 12 of our opposition. That does speak of potential financial harm. That's an additional theory that we believe also shows our standing here. But that's been, we believe, adequately discussed earlier in this hearing.

THE COURT: All right. Okay.

Well, thank you very much. Thank you, everybody. And as I said, I think it's useful to hear some discussion about some of the other merits-based attacks on the complaint.

So we'll get back together on November 10 at 9:30 and address the legal challenges to the APA claim and the Tucker Act claim and some of the other claims. And so I'll

see you then. All right. Thank you.

* * *

CERTIFICATE OF OFFICIAL COURT REPORTER

I, JANICE DICKMAN, do hereby certify that the above and foregoing constitutes a true and accurate transcript of my stenograph notes and is a full, true and complete transcript of the proceedings to the best of my ability.

Dated this 28th day of October, 2016.

/s/_____

Janice E. Dickman, CRR, RMR
Official Court Reporter
Room 6523
333 Constitution Avenue NW
Washington, D.C. 20001

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

In re: U.S. Office of Personnel Management Data Security Breach Litigation,	) Civil Action) No. 15-mc-1394)) MOTIONS HEARING)) Washington, DC) November 10, 2016) Time: 9:30 A.M.)

TRANSCRIPT OF MOTIONS HEARING
HELD BEFORE
THE HONORABLE JUDGE AMY BERMAN JACKSON
UNITED STATES DISTRICT JUDGE

A P P E A R A N C E S

For the Plaintiffs:

Daniel Girard, Esq.
Jordan Elias, Esq.
Girard, Gibbs
601 California Street
14th Floor
San Francisco, CA 94108

Peter A. Patterson, Esq.
Cooper & Kirk
1523 New Hampshire Avenue N.W.
Washington, DC 20036

Tina Wolfson, Esq.
Ahdoot & Wolfson, PC
1016 Palm Avenue
West Hollywood, CA 900069

Paras Shah, Esq.
Bredhoff & Kaiser
805 Fifteenth Street N.W.
Washington, DC 20005

Government Counsel:	**Matthew A. Josephson, Esq.** U.S. Department of Justice Civil Division 20 Massachusetts Avenue N.W. Washington, DC 20530
KeyPoint Counsel:	**Jason J. Mendro, Esq.** Gibson, Dunn & Crutcher 1050 Connecticut Avenue N.W. Washington, DC 20036

Court Reporter:	Janice E. Dickman, RMR, CRR Official Court Reporter United States Courthouse, Room 6523 333 Constitution Avenue, NW Washington, DC 20001 202-354-3267

* * * * * * * P R O C E E D I N G S * * * * * * *

THE COURTROOM DEPUTY: Your Honor, calling miscellaneous case number 15-1394, In re: United States Office of Personnel Management Data Security Breach Litigation.

Will arguing counsel please approach the lectern, identify yourself and your colleagues for the record.

MR. JOSEPHSON: Good morning, Your Honor. Matt Josephson on behalf of the Office of Personnel Management. With me at counsel table I have Elizabeth Shapiro, Drew Carmichael and Joseph Borson.

THE COURT: All right. Thank you.

MR. GIRARD: Good morning, Your Honor. Dan Girard on behalf of the class plaintiffs.

MR. ELIAS: Good morning. Jordan Elias for the class plaintiffs.

MS. WOLFSON: Good morning, Your Honor. Tina Wolfson for the plaintiffs.

THE COURT: Good morning. I think it's the first time I've seen you live.

MS. WOLFSON: It's a pleasure to be here.

MR. PATTERSON: Good morning. Pete Patterson for the class plaintiffs.

MR. SHAH: Good morning, Your Honor. Paras Shah for NTEU plaintiffs. With me is Gregory O'Duden, General

Counsel, Larry Adkins, Deputy General Counsel, and Allie Giles.

THE COURT: All right. Good morning.

MR. MENDRO: Good morning, Your Honor. Jason Mendro, from Gibson, Dunn, on behalf of KeyPoint Government Solutions this morning, here with my colleagues Scott Richardson, Jeremy Christiansen, and Robyn Schechter.

THE COURT: All right. We certainly have enough people here. Good morning, everyone.

I want to start out by saying that I have a read the pleadings and I understand the issues and I think -- I mean, the point, counterpoint was excellent. I know exactly what your positions are and what cases you're replying upon. So I don't expect to be as active as I was last week.

But, if I do go on to the merits on some or all of these claims, I want to make sure that I've given everyone the opportunity to give me their best argument to point me to the particular points you want to highlight and you want me to focus on. And because, in my experience, oral argument -- preparing for oral argument often focuses the mind in a way that writing a brief does not. If you have something that's more clear or slightly different that you want to tell me, a better way of putting things, I want to hear it.

So, I want to go through each of the claims with

each of the parties, just to make sure I have your latest and best thinking on them, and then I'm going to take the entire matter under advisement.

So, let me start with counsel for OPM, since you are the moving party here. And notwithstanding everything I just said, I do want to ask a preliminary question first. And that is, is the actual damages issue that we talked about under the privacy act last time a standing issue or a 12(b)(6) issue? *Cooper* analyzed it as a waiver of sovereign immunity and didn't specify any particular federal rule. But it seems to me that would be a 12(b)(1) issue. So I just want to know how you conceived of the whole thing.

MR. JOSEPHSON: There's not a lot of case law on exactly what rule that would fall under. It is an element of a Privacy Act claim, which may suggest that it's more of a 12(b)(6) matter. But, it is true that it's a -- Privacy Act is a waiver of sovereign immunity, so in that sense if you don't meet that element, the waiver wouldn't apply, which would make it more of a 12(b)(1) issue.

For purposes of this motion, I don't think it's a material distinction. That would only really come up if there were, you know, any kind of waiver question or something of that nature. So I don't think the precise procedural rule would be material to the disposition of the motion. So we did not specify in our papers, really because

there is no -- no law on that yet.

THE COURT: Okay. You know, I started wrestling with it and ultimately I went back to *Cooper* and *Cooper* specifically talks about it as a sovereign immunity issue, and other case law says sovereign immunity is a subject matter jurisdiction issue, and that's with respect to actual damages. I suppose it may also apply to the sustained-as-a-result-of part of the test. I'm not sure.

But my question for you is is the causation test under the Privacy Act for what something has been sustained as-a-result-of different or the same as the test for causation fairly traceable under the causation prong of Article III standing?

MR. JOSEPHSON: Causation for purposes of the Privacy Act is more stringent than causation for purposes of Article III. The cases in the Article III context often talk about the fairly traceable element as something less than proximate cause or something around proximate cause. But when you're talking about the Privacy Act, which is a waiver of sovereign immunity, it has to be strictly construed and that causal link is more of a but-for requirement.

THE COURT: And --

MR. JOSEPHSON: Closer to tort causation.

THE COURT: Are there cases that say that?

MR. JOSEPHSON: There are --we cite in our

pleadings, there's a D.C. Circuit case that sort of -- it predates *Cooper*, but it uses the sovereign immunity cannon to go through the elements of a Privacy Act claim. And there the Court looks at -- the issue in that case was how do we describe -- or, in instance of disclosure, do we narrowly define it, broadly define it?

It wasn't a causation case, but the same principle would apply when you're analyzing the elements of a waiver of sovereign immunity. Each element would have to be construed narrowly and if there's any ambiguity about whether a particular theory would fall under a particular element, tie goes to the United States. And that's what Justice Alito said in *Cooper*, if there's any ambiguity on this question, the waiver would bar the -- the waiver wouldn't apply and the claim would be precluded.

THE COURT: All right. I understand that, that *Cooper* stands for that proposition, but just the specific that it would be a but-for test, is there any opinion that you're relying on for that, or you're saying that that is strict causation, so it must be a but-for test?

MR. JOSEPHSON: I think the best place to start is the statute itself, which does require that the actual damages are caused by the particular violation that's alleged, which is definitely more than the more nebulous fairly-traceable language that's in Article III cases. I

think that that is the state of the law, that the statutory language -- it's a matter of construing the statutory language and applying the teachings of *Cooper*, which requires a sovereign immunity cannon type analysis and narrowly construing each element. And I think that that's the state of the law at the time -- at this time.

THE COURT: Okay. All right. So with that, now we are -- and we talked about actual damages last time so I don't think we need to talk about them again, but we hadn't talked about sustained-as-a-result-of, so I wanted to hear you on that.

So let's go on to the merits of the disclosure and the failure to establish standards claims under the Privacy Act.

MR. JOSEPHSON: You would like to start with the Privacy Act claim itself?

THE COURT: Well, you can start wherever you want, but since we're already talking about the Privacy Act and I have it written down first, that would be helpful.

MR. JOSEPHSON: Sure. Plaintiffs have two Privacy Act claims. A disclosure claim under 552a(b) and then a safeguards claim under (e)(9).

With respect to the disclosure claim, there cannot be, as the *VA Data Breach* case that we've cited in our pleadings explains, there cannot be an intentional and

willful disclosure by the agency when the legal theory is that a third-party acted in an intentional or willful fashion in breaching a particular cybersecurity defense. Does not fit the statutory language. In the Privacy Act there's been no intentional disclosure by the Agency to another person or to another agency, which is what the Privacy Act precludes.

So the disclosure claim fails for that purely legal reason, that threshold reason.

The safeguards claim, similarly -- the first point I would emphasize is the standard of culpability under the Privacy Act is very high. It's -- as the Circuit has explained, in order to state a claim for money damages under the Act, which is the claim at issue here, a plaintiff must plead facts establishing patently egregious conduct or conduct that is beyond grossly negligent.

THE COURT: Well, do you agree, though, that one acceptable interpretation of the standard is, quote, somewhat greater than gross negligence?

MR. JOSEPHSON: That's true. It's got to be greater than gross negligence. Now, but gross negligence is itself a very high bar, and so to plead -- the plaintiff has the burden of pleading facts that would jump that hurdle, which is quite high.

THE COURT: Well, if I have to construe all the

inferences in the complaint in plaintiffs' favor and take all the allegations as true, how can I find, as a matter of law at this stage, that the failure to establish safeguards didn't rise to the level of more than gross negligence? I mean, isn't this case similar to Judge Robertson in the *VA Data Theft* case where it was the same thing, a failure to establish appropriate standards, notwithstanding being on notice of the need for them. And he said, you know, at least at the 12(b)(6) stage they state that -- that had stated a claim for willful.

MR. JOSEPHSON: For the Privacy Act claim we would -- the clearest, most straightforward basis for dismissal is the actual damages issue. I think that is -- that is clear. And for the disclosure claim, their theory of the case just doesn't fit that provision.

The question is closer on the pleadings for the safeguards claim. We would definitely agree with that, about whether -- what's the best procedural way to address those types of allegations.

THE COURT: I mean, because it struck me that if I were to hold that this complaint doesn't rise to the level of a willful violation of the adequate safeguards provision, that what you're telling me is that there really could never be an actual actionable claim under the safeguards provision. But Congress clearly gave private parties the

right to sue under that provision.

MR. JOSEPHSON: I don't think that the ruling we're asking for would be -- preclude all theories. Our argument is that in this case, when the allegations are that a third party acted in a sophisticated and malicious fashion to breach an agency's safeguards, that you've now created a more -- a higher burden than originally, and the burden was already high. I mean, it's now -- you're asking for a ruling that the agency should have precluded, which by their own allegations was sophisticated and malicious conduct. It's a very difficult theory of the case for the Privacy Act.

But even in the Court were to hold that for purposes of pleading the safeguards claim, stated claim, the actual damages issue would get rid of all Privacy Act claims.

THE COURT: Right. Well, since the Privacy Act doesn't include equitable relief, how does the Privacy Act bar a claim for equitable relief under the APA?

MR. JOSEPHSON: Because under section 702 of the APA, the APA does not apply if another statute expressly or impliedly forbids the relief which is sought. And here the Privacy Act forbids the injunctive relief sought because it contains a very detailed remedial scheme that carefully links the remedy available to the violation alleged.

If you look at 552a(g), which is the civil remedy provision, it carefully lays out the claims, as well as what

remedy is available for that particular claim. When you look at that section it's very clear that injunctive relief is only available for amendment claims and access claims, claims where plaintiff is seeking the court to change a federal record or seeking access to it. There is no injunctive relief for the catch-all provision, which is what plaintiffs have sued here -- sued under here in this case.

As the courts in this District have explained and as the Ninth, Tenth, and Eleventh Circuits have explained, when you have a very detailed remedial scheme like the Privacy Act, that itself precludes the broader injunctive relief that's available under the APA when you look at 702 of the APA.

Now, the plaintiffs have argued that the Privacy Act does not preclude the APA because its remedial scheme is inadequate. But the point is that that's precisely -- those are precisely the remedies that Congress intended a plaintiff to get for these types of claims. And I think the analysis in the *Cell Associates versus NIH* case, it's the Ninth Circuit case which came out shortly after the Privacy Act was enacted, just four years after it was enacted, the Court goes through the analysis, the plain language analysis, and says these are remedies available for these claims. We're going to assume Congress intended to -- meant what it said and intended those to be the remedies. And

they also go through the legislative history and they look at the House report and Senate report. And there's actually evidence in the legislative history that these were the only remedies that Congress intended a plaintiff to get for these types of claims. I think it's a great case in terms of going through the analysis.

THE COURT: If I agree with you on that, do I still have to consider the FISMA as the basis for the illegality or the decisions? I think your argument is that there there's no concrete decision and there's no standards to apply and so the APA doesn't apply. But, I still have to reach that issue, don't I, even if I agree with you about the Privacy Act barring remedies for this? Or don't I?

MR. JOSEPHSON: I think in this case plaintiffs have cited FISMA as evidence of the safeguards that are -- that they think are required or appropriate under the Privacy Act. I don't read the complaint as asserting a separate theory of enforcing a particular FISMA position -- provision outside of the Privacy Act. For purposes of the preclusion analysis, I think the operative question is do the allegations fit within the scheme Congress has created? And if the answer is yes, then these are the remedies you get. And I think that the reliance on FISMA, plaintiffs' reliance on FISMA quite clearly falls within the scope of the Privacy Act because they're all safeguard type

provisions that would -- that are being used to state a Safeguards Privacy Act claim. So I think a preclusion analysis gets -- requires dismissal of the entire thing.

THE COURT: But you spend a lot of time attacking it, and sort of the ordinary attack on an APA claim on the grounds that there's no decision and that the decision is subject to agency discretion and, therefore, not reviewable because there aren't standards within the statute.

So, are you saying I just really don't have to get to that? You only put that in there if I don't agree with you about preclusion, or --

MR. JOSEPHSON: Alternative basis for dismissal. I think preclusion requires dismissal of the whole claim. To the extent plaintiffs are trying to assert an alternative claim under FISMA, trying to enforce a FISMA provision separate and apart from the Privacy Act, I think that argument fails because if the claim falls within the ambit of the Privacy Act, it's precluded pursuant to section 702 of the APA.

But if the Court were to disagree with that position and consider the FISMA claim separate, it would be -- it would dismissed -- it should be dismissed based on the committed agency discretion argument, as well as the final and discrete agency action argument we make in the pleadings.

On those points I just want to highlight a couple things. With respect to the committed to agency discretion argument, I'd start by staying FISMA is a new statute, fairly new statute, and it has been recently amended, so when you do research on this, there's not a lot of cases out there that are going to explain the provisions and its structure. This is an analysis that -- it's got to be done in the first instance. So this is a new area of the law.

But when you look at the language and the structure of the statute itself, there are a couple of things that jump out at you. And the D.C. Circuit has some very -- is probably the best case that I've found on this, where they go through FISMA -- and this is pre-amendment, but most of the provisions are the same -- they go through the statute and the *Cobell* case that we cite in our papers and they point out that the statute is multilayered and assigns responsibility for implementation and compliance to a host of entities across the executive branch.

It's unique in that respect, where one agency has responsibility for monitoring another agency, agency's compliance with IT rules and regs. It specifically, the Office of Management and Budget has the exclusive responsibility under that statute to make sure other agencies are complying with applicable directives.

In addition to the multilayered nature of the

statute, FISMA does not prescribe specific methods or tools for ensuring the safety of data. It lays out general requirements. For example, the statute requires agencies to adopt security protections commensurate with the risk and magnitude of the harm under 3554(a)(1)(A), but it does not say what protections must be implemented, nor does it tell agencies how to balance the risk or what to adopt.

It's true, and the plaintiffs' rely on these directives in their opposition, there are directives that implement FISMA that do require specific things, like Homeland Security Presidential Directive 12, OMB Memorandum M-11-11 and the FIPS publications. The one the plaintiffs cite is 201-2, along with the OMB memoranda 11-11. There's a host of these types of memoranda and implementing provisions that have specific requirements for specific systems, but those directives specifically say they're not judicially enforceable in federal court, which we point out in our reply. Or they make clear on the document that OMB is the agency responsible for ensuring compliance with the directives.

So when you look at the language and the structure of the statute, there's no real role for the judicial branch to play. And that's exactly what the D.C. Circuit said in the *Cobell* case. Granted, it was dicta, it was not the issue before the Court, but it certainly is persuasive in

interpreting the statute.

In addition to the 701(a)(2) committed agency discretion argument, we've also argued that plaintiffs have failed to identify discrete agency action under 706 of the APA.

And I want to highlight two aspects of the argument. One, the relief requested shows that the plaintiffs have failed to identify discrete and final agency action. When you look at the prayer for relief, specifically subsection -- or, paragraph F, plaintiffs ask the Court to, quote, formally adopt -- to order OPM to, quote, formulate, adopt, and implement a data security plan that complies with FISMA and the Privacy Act. That's precisely the type of relief that the Supreme Court said in *Southern Utah* that's not appropriate under the APA.

In addition to the relief requested, the very nature of the claim shows that it's not susceptible to judicial resolution under the APA. When you look at the particular agency actions that the plaintiffs are asking the Court to enforce, they're very clear that the Court cannot resolve these types of issues in this forum.

Number one, just as examples, plaintiffs take issue with OPM's operation of systems without valid authorizations. No standard is set forth on how the Court could evaluate whether a particular system is being operated

according to a valid authorization. Plaintiffs take issue with the multifactor authentication process that OPM uses for particular systems. No judicial standard about how the Court could determined whether one system requires multifactor authentication or if another does not, or if there are exceptions to that rule. Adequate network and data segmentation, use of firewalls and host-level malware, proper encryption levels, these are precisely the type of agency -- or, purported agency actions that the Supreme Court has said are not judicially reviewable because they would entangle the Court in the day-to-day management of OPM's information security program. It would effectively turn the Court into an information security tribunal where the Court would then have the responsibility for deciding what is appropriate data security under FISMA or what is not. And that's precluded by *Southern Utah*.

In their opposition plaintiffs actually, I think, implicitly acknowledge the unworkability of the claim when they say that the Court could issue a special master to oversee the data compliance of -- oversee OPM's data compliance. But of course the special master can't exceed the powers of the Court that appointed it, and so that request really just goes to show the lack of discrete agency action in the case.

With respect to the Little Tucker Act, there's no

contract here with the United States, no element of a contract has been alleged. I think the most straightforward element lacking is consideration. The promise to perform a preexisting legal duty cannot form a contract, and that's precisely what plaintiffs have identified in the complaint.

They point to a disclosure statement on the SF-86 and the SF-85 that notifies the applicant that the information will be treated consistent with the Privacy Act. That's it. There's been no -- there's no contract above and beyond the Privacy Act, it just notifies the applicant that the information will be treated consistent with that federal statute. If the applicant thinks the information is not treated consistent with the federal statute, then they can sue under that particular federal statute. But they cannot, under a contractual theory, bypass that statute and sue in contract.

Plaintiffs rely on a host of data breach cases involving private entities selling services or goods where the Courts, in those cases, concluded that there is a bargain for exchange with respect to data security obligations. Of course, that hasn't happened here. This is an employment situation involving a standard government form filled out as a condition of employment. There's no bargain for consideration for data security or anything else.

With respect to the constitutional claim we go

through the Supreme Court cases that discuss the constitutional right to informational privacy; I won't go into the details of those cases. But we do highlight the three limitations that we think preclude any claim in this particular case. Namely, all three of those cases concerned potential constitutional limits on the government's authority to collect information from individuals. At no point did the Supreme Court ever hold or suggest that there's an affirmative duty to protect the data from third-party harm.

Second, and most recently, in the *NASA v Nelson* case the Supreme Court made clear that statutory protections, including the Privacy Act, specifically can allay any constitutional privacy rights, even if the individual may be affected by data breach at a federal agency.

And finally, the Supreme Court relied on the fact that the government has considerable deference as an employer in implementing its data security program, more deference than it would have if it were exercising its sovereign authority to regulate a particular matter.

So all three of those factors preclude plaintiffs' attempt to constitutionalize data security in this case.

The reason the Supreme Court has never suggested that there's an affirmative constitutional duty to protect

data from third-party harm is because that holding would itself conflict with other substantive due process cases which hold there is no duty to protect individuals from third-party harm. That's *DeShaney versus Winnebago County*.

There is a very limited exception in *DeShaney* for situations when the government has placed an individual in physical custody. At that point an affirmative constitutional duty to provide basic services, basic -- to provide for one's basic human needs does arise. But the custody of data isn't physical custody, nor does the government's control of data deprive anyone of liberty under the due process clause.

So the *DeShaney* -- the *DeShaney* exception is clearly inapplicable here. And the plaintiffs cite various circuit cases, *Fadjo*, *Eagle*, and *Sheets* in support of their novel constitutional theory. But all of those cases concern situations where state actors deliberately and intentionally released information, private personal information to another person or to the public. A deliberate disclosure. And the circuits did, in those cases, extrapolate from the informational privacy cases from the Supreme Court and say there has been an intentional or willful disclosure by the government, it's personal information, there may be a constitutional protection there, and they found that those allegations stated a viable claim.

No intentional disclosure by the government here. Instead, the theory is that OPM had a constitutional duty to protect data from a third party, which is clearly precluded by *DeShaney* and is not supported by the informational privacy cases.

Final point, to state a substantive due process claim you have to plead contact that shocks the conscience. Only abuses of executive power, state claims under the substantive due -- component of the due process clause. The due process clause is not a font of tort law, as the Supreme Court has said many times. And under *City of Sacramento versus Lewis* and the D.C. Circuit decision implementing that case, *Fraternal Order of Police versus Williams*, large scale personnel and program decisions made by government officials do not rise to the level of conscience-shocking behavior. Therefore, plaintiffs have not stated a claim for that additional reason.

Unless the Court has any other questions, that will conclude --

THE COURT: All right. Thank you. All right. Let me start -- I don't know how you all have divided this up, but I would like to start with the Privacy Act of the plaintiffs, then we'll do the contract claim, then we'll do the APA.

Good morning.

MR. PATTERSON: Good morning, Your Honor.

THE COURT: What is your position on whether the actual damages issue that we talked about last time is a 12(b)(6) issue or a standing jurisdictional issue?

MR. PATTERSON: First having thought of it, but it seems to me that it could be -- should be a 12(b)(6) issue, since it's, as opposing counsel mentioned, it's an element of the claim versus --

THE COURT: Once the Supreme Court has characterized as a sovereign immunity issue, doesn't that make it a 12(b)(1) issue?

MR. PATTERSON: Yes.

THE COURT: I realize this is all very esoterical.

MR. PATTERSON: Yes.

THE COURT: I have seen circuit court opinions that point out the district court didn't even identify the rule under which they were ruling, so I'm going to identify the rule under which I'm ruling. And it also affects whether you base it only on the face of the complaint, whether you consider other information. I mean, it does affect the standard to be applied.

And it seems to me I originally conceived it of, okay, first I have to find standing and then I go to 12(b)(6) merits or the actual damages sustained as a result of. Then I read *Cooper* and I realize that you're probably

still in the 12(b)(1) world. But you haven't devoted a lot of time to figuring those out.

MR. PATTERSON: Right. One thought is, you know, that *Cooper* established that you have to show, you know, alleged pecuniary harm under that provision. So maybe the question of what you have to -- you know, what types of harm are cognizable under that, perhaps that's a 12(b)(1) question. But then when you are alleging these are pecuniary harms and we've done these things, you know, whether those are valid allegations, perhaps that's a 12(b)(6) question, would be one way to divide it.

THE COURT: And we talked last time about whether you have or you haven't alleged monetary harm. And I don't think we need to replow that ground. But, are there cases that, in your view, detail what's necessary for sustained-as-a-result-of? What is the test for causation under the damages provision?

MR. PATTERSON: I think the *Hill* case is a case from this court that we cited, says that the plaintiffs need to plausibly allege proximate causation, and proximate causation just is something that, you know, reasonably is attributable to the action that was taken. So I think that -- that's the one case I know that we've cited that's been cited in the briefs that talked about that.

THE COURT: All right. Well, let's talk about

whether theft by a third party, a sophisticated and malicious breach is an actionable disclosure. You cite the *Beaven* case, which doesn't strike me as being nearly as analogous as the *VA Data Theft* case which you relied on for standing and which was based on the exact thing you're saying here, which is the defendants ignored warnings that the Agency's data was vulnerable. And Judge Robertson said that works for adequate safeguards, it doesn't rise to willfulness for disclosure purposes. So why was he wrong about that?

MR. PATTERSON: Well, I think we were citing *Beaven* to combat the government's assertion that since this was a third party that came in and stole it or took it, the actual disclosure, the final act, if you will, was not intentional or willful. And *Beaven* explains why that's not so. But I think it is fair to say that this really, under the Privacy Act, it rises or falls with the adequate safeguards. Because if there were adequate safeguards, then I don't see how we could say the disclosure was intentional and willful.

THE COURT: It seems to me you were conflating them.

MR. PATTERSON: Yes.

THE COURT: And your disclosure was just a repetition of, well, they didn't have safeguards.

MR. PATTERSON: Yeah. And the answer could be,

well, you know, if there weren't inadequate safeguards, then the disclosure is also actionable. So maybe that conflation is not improper. But even if -- regardless of which way you look at it, I think it does depend on us, you know, meeting the requirement that the adequate safeguards provision was not met.

And I think for those purposes, under the *VA Data Theft Litigation* and in *Holly* (ph.), I mean, we have a lot more here in terms of, you know, nearly a decade's worth of warnings and admonishments from the IG on precisely the issues that perhaps caused this breach or allowed this breach to happen, whereas in those cases there wasn't, you know, as lengthy or detailed a history of a problem and it was not, you know, as tightly connected to what actually happened in those cases.

So, if there was willful and intentional conduct in those cases, and you're going to agree with those -- the reasoning of those cases, I think it follows that there is here as well.

THE COURT: Well, if the source of a good part of your argument that their safeguards were inadequate is that they failed to comply with FISMA and FISMA specifically does not have a private right of action attached to it, how is it consistent with the principles of sovereign immunity to say we're going to hold you responsible under the Privacy Act

for not -- or, the APA for not complying with FISMA when Congress didn't waive sovereign immunity in FISMA?

MR. PATTERSON: Well, I mean, if Congress does not have a private right of action in the statute, that just means the APA is available to enforce the agency's obligations under law. So the fact that there's not a private right of action under FISMA -- you know, we're not asserting a cause of action under FISMA, we're asserting it under the APA, which is a stopgap for all agency obligations.

THE COURT: Was the government counsel correct when he read your complaint to not be asserting FISMA as a separate source of APA review? That what you're saying under the APA, is that we're entitled to injunctive relief, that the Privacy Act doesn't provide, under the APA, for violating the Privacy Act. Or are you saying specifically that we're entitled to injunctive relief under the APA for violating FISMA?

MR. PATTERSON: The way I can see that is that we're doing both. We're saying that under the APA you can enforce the Privacy Act, and also under the APA you can enforce FISMA. And the third thing, also, I think that the FISMA requirements can inform what the Agency was required to do or should be required to do even under the Privacy Act. So, you know, I don't think we're limiting ourselves in that way.

THE COURT: Well, if the Privacy Act specifically said, with respect to the failure to maintain adequate safeguards, we are letting you sue for damages, if you've been actually harmed by this, you're entitled to collect, but, no, we're not giving you a right to sue for injunctive relief. Why doesn't that preclude trying to squeeze it in through the APA after Congress -- because doesn't that put me in the position of becoming the super-overseer IT professional for the executive branch, which it seems like the Privacy Act specifically said we're not going to let you do that, Court, if you just give damages to people who are harmed. You can't give broad prophylactic relief.

MR. PATTERSON: Well, a few points on that. First, in the *Doe versus Stephens* case the D.C. Circuit has already held that the Privacy Act can be enforced through the APA. In that case it was about --

THE COURT: Well, that was a discrete act of unlawful disclosure of a particular veteran's records in violation of the Act. And so I don't really think that's analogous to the entire design and management of the agency's security system.

MR. PATTERSON: Yeah, and it's not -- but that's -- think that answers the question, though, of whether the APA -- or, the Privacy Act precludes APA relief; full stop. Because if it did, *Doe versus Stephens* would have come out

the other way.

So I think what the Court is getting at now is kind of the *Southern Utah Wilderness* discrete and agency action that's required. And, you know, I admit the complaint is pleaded very broadly, but I think there are some discrete actions that we think the Court should focus on.

One is -- and the principle one, the main one, is this operating systems without a required authorization. And this is not something that is optional, as these IG reports make clear. Under FISMA -- and just to back up a little bit, under FISMA, under 44 U.S.C. 354(a)(1) [sic], it says: The head of each agency shall be responsible for complying with certain requirements, including those promulgations by the OMB director, secretary of Homeland Security, and so forth. And then the -- you know, the OMB director has said, I believe it's in Circular A-130, Appendix III that we've cited, has said that you have to have valid authorizations before you operate your systems and you have to reauthorize them every three years. And they've not done that.

So, you know, it's not that you have to manage their whole IT department -- although I admit that some of the language in the complaint is drafted that way -- but, you know, we would urge not to throw out the baby with the bath water, so to speak, and that we've got some claims of,

you know, operating things with lack of authorization, inadequate training, not even having an inventory of the devices and things that are hooked up to the system which precludes them from, by definition, from knowing whether things are secure.

So there are some very discrete actions that Your Honor could order the agency to take, and then it's just have they done it or haven't they done it? It's not that you're managing their IT system.

THE COURT: What's your response to their argument that those specific discrete actions that you've pulled from these memoranda and regulations that implement FISMA, that those documents themselves specifically indicate they're not subject to judicial review?

MR. PATTERSON: Well, the only document that says that I believe is the H -- HSPD-12, I believe is the one it was. The one that said you have to have multifactor authentication. But then after that OMB, in the M-11-11 document says, Agencies, you have to follow this. And under FISMA, the provision that I quoted to you, it says the head of each agency shall be responsible for complying with these requirements. And then as the Agency says, including directives from OMB, and that if OMB says you have to do these things, well, under statute that's an obligation, that's not something that is optional.

And then the *Southern Utah Wilderness* case, again, that they cited talked about the Bureau of Land Management. And it said the statutory directive that BLM manage in accordance with land use plans and the regulatory requirement that authorizations and actions conform to those plans prevent BLM from taking actions inconsistent with the provisions of a land use plan. And the case went the other way there because the language in -- that the plaintiffs were trying to enforce was not sufficiently direct and discrete and binding enough for the Court to say we can enforce it.

But that's different here where they've said no, you have to do these things with respect to authorizations, for example. And under the statute, those are binding on the agency and they're required to do them.

THE COURT: So -- and I know in your brief you set out the things that you think are sufficiently specific and discrete for me to order them to do them if I have authority under the APA to do that.

MR. PATTERSON: Yes.

THE COURT: So that's where I would find that there's not any others that you want to focus me on. Those are the ones that I should look at to see if they're sufficiently discrete and reviewable. And you say they're reviewable because of the provision in the FISMA that says

the agency shall comply with them.

MR. PATTERSON: Yes.

THE COURT: All right. Now, what do you make of the D.C. Circuit's observations in *Cobell* about the reviewability of FISMA decisions?

MR. PATTERSON: Well, it was, admittedly, dicta, and I don't think the Court focused on -- I think the Court focused on kind of the broad -- you know, the head of OMB should develop certain policies and procedures and didn't get down to the level of, okay, after the head of OMB has done that and identified certain discrete things that agencies are required to do at that point, is could there be a cause of action? Because I think we would admit if we were coming in here against director of OMB and saying, well, these policies and procedures he's adopted are not adequate to meet the purposes of FISMA, that would be a different thing. But what we're saying is that, you know, they have decided on certain actions that are required under FISMA.

So all we're asking you to do is to say that things that the government has determined is required under FISMA, that they follow those things that they've already determined is required under FISMA. So it's not -- we're not trying to displace the government's discretion, we're just trying to say, okay, once they've come at their answer,

the statute says they have to follow through.

THE COURT: But, let's say I disagree with you about the *Doe v. Stephens* intended to or did say what you say it says, I want to go back to the question of if the Privacy Act specifically excludes the kind of relief you're talking about for the failure to maintain safeguards, which is really the heart of your APA claim, why doesn't that have preclusive effect?

I mean, it seems to me Congress is saying we're going to leave the internal workings of the government to the government. If you're harmed by it, you can see them and you can be compensated for your harm. But the judiciary is not going to run the executive branch in its internal machinations.

MR. PATTERSON: Two things I want say to that. One about the Privacy Act itself and then one about FISMA independently.

So on the Privacy Act, Congress didn't specifically say you can't get this relief. What it did do is it said, you know, here's a cause of action and here are certain causes of relief you can get. So then you have to ask the question, well, did Congress intend to preclude other sorts of claims under the APA or was Congress just meaning to set out specific relief you can get under the Privacy Act and then have the presumption that the APA

backstops that kick in as well.

And as *Garcia versus Vilsack* from the D.C. Circuit makes clear, that we've cited, you have to have clear and convincing evidence that Congress intended to preclude another, you know, APA cause of action. And that's just not present on the face of the statute. There are a couple equitable relief claims that are allowed. But the reason for those is because they differ from the APA relief; there's exhaustion requirements, there are -- there's a limited -- statutes of limitations under the Privacy Act that's shorter than under the APA, there's a smaller class of people that can get relief under the Privacy Act than under the APA.

So for those claims, if someone comes into court -- and this is what many of the cases they've cited have held -- and said, for example, under the APA I want to get my record amended but now it's four years afterward and I didn't go through the exhaustion procedure and I'm not an American citizen, the Courts say, well, Congress has established that specific relief under the APA and if you don't meet -- under the Privacy Act and if you don't meet those requirements, you can't use the APA as an end run.

Here, that's not the case here where Congress has just been silent on equitable relief for the type of claim we're asserting and there's no inference that can be drawn

that they attempted to displace the APA.

THE COURT: If you're talking about sovereign immunity, isn't the inference that if they didn't say you can't do it, you can't do it?

MR. PATTERSON: No, because the APA is a waiver. So the presumption is actually reversed because for equitable relief the APA is a waiver of sovereign immunity.

THE COURT: Unless there's a statute that deals comprehensively with the issue. The Privacy Act deals comprehensibly with the issue. It sets out what remedies you can have, what remedies you can't have.

MR. PATTERSON: Right. Right. And you have to have clear and convincing evidence that those remedies that they set out intended to foreclose the APA cause of action, which has always been held to -- supposed to have expansive interpretation, not limited interpretation. And there's a strong presumption that agency actions are subject to review. That's what the Supreme Court in the *Doe v. Chao* case, in the footnote 1 said, well, it acts to, I think, implicitly address the dissents' argument that you're gutting the Privacy Act.

They said, you know, well, perhaps the reason that there's no equitable claim, you know, provision for these sorts of claims is that Congress expected the APA provisions to be there, citing the District Court case -- decision in

that case. And the District Court had said we're not going to assume that Congress intended to allow agencies to run roughshod over people's rights under the Privacy Act and let -- have the people have nothing to do about it except this damages claim for relief. So --

THE COURT: Well, again, when you're talking about running roughshod, you're talking about intentional acts and disclosure type things. Here we're talking about the failure to maintain adequate safeguards. It's an internal management system. And you say no, there are requirements, at least in some circulars issued by OMB or Homeland Security, other materials that specifically say what an agency is supposed to do. And since the statute FISMA says the head of the agency is responsible for complying with them, there's enough specificity for me to hold the Agency's feet to the fire. But where's the decision that gives me jurisdiction under the APA to look at a failure to comply with an OMB Circular guidance on what authority should be? What's the decision?

MR. PATTERSON: Well, under 706(a)(1) or (2), I forget which one it is now, but you have authority to compel agency action unlawfully withheld or, you know, final agency action. So it's whether you look it as the action was putting these systems into operation without valid authorization, you know, that's either -- that's an action,

or it's also an action withheld, that you're supposed to authorize these things, and they haven't done that. So either way, I mean, it's either they've taken these discrete actions --

THE COURT: Other than *Doe v. Stephens*, do you have any case that suggests that the, sort of, Agency's internal management of itself and its security systems or its data systems, or really anything else, even its employment rules, is the kind of decision that we're even talking about when we talk about the APA?

MR. PATTERSON: I don't know -- well, I think even the *Southern Utah Wilderness* case which dealt with land management, but as I said --

THE COURT: That is an agency that is tasked with land management.

MR. PATTERSON: Okay. And OPM is tasked with securing our information.

THE COURT: It's tasked with gathering it and processing it for certain reasons, to decide who's going to get hired and not hired. And it has a corresponding obligation to keep what it has secure. But it isn't the Department of Secure Data department.

MR. PATTERSON: Right.

THE COURT: That's not its task, that's its operational responsibility. To me there's something

different between failing to operate under the standards that the government has set for itself to operate under that aren't set out in the statute, except the Privacy Act which says -- doesn't provide for relief and calling that a decision that's committed to the Agency that's reviewable under the APA.

MR. PATTERSON: Well --

THE COURT: You're saying that somebody made a decision not to comply with OMB Circular such and such. So where is the record of that decision? Where is the underlying material that I would -- I mean, when I review an agency decision I have to decide based on the record. So I have to look at everything that was before the Agency when it made its decision, and was that decision rationally based on that record, not did I like the decision and would I have made a different decision. So how do any of the decisions you have fall within that rubric?

MR. PATTERSON: Well, it would be the Agency's responsibility to produce an administrative record.

THE COURT: Well, how would there be an administrative record of the decision, the decision to have inadequate training?

MR. PATTERSON: Well, they -- someone made a decision to allow employees to not fulfil their obligations. I mean, the APA says you can order action unlawfully

withheld. So they're required to do certain training.

Now, you know, the record is going to look a little bit different in a case, I think, when it's action unlawfully withheld, because the whole point is that they didn't do something.

So, you know, I think -- I don't know -- I'm not sure what the record is going to look like, if they're going to have materials that says this is why we decided to withhold this action, or maybe it's just they didn't have anything.

THE COURT: All the cases, I mean, they are difficult, but they're eased somewhat by the clarity of the action that's being requested, and it can't be something that's completely committed to their discretion, it has to be something they must do.

MR. PATTERSON: And here I think you can't, so the committed-to-their-discretion is saying there's no law to apply. You know, the Court can't decide what they're supposed to do. But here, by the fact that Congress has created a damages cause of action, there's no question that there's law to apply because by doing that it's saying, well, the courts can determine whether there were adequate safeguards.

THE COURT: And you're pointing to agency materials, not the statute itself, for the standard against

which I'm supposed to measure the decisions that you challenge in paragraph 200 and thereafter. Is there any language that you can point to in the statute that suggests that the development and implementation of a security system that meets the requirements that you think they should meet is not a matter committed to agency discretion? Where are the statutory standards I'm supposed to rely on?

MR. PATTERSON: Right. So it's 44 U.S.C. 3554(a)(1)(B).

THE COURT: Do you want to say that again?

MR. PATTERSON: It's 44 U.S.C. 3554(a)(1)(B) that says the head of each agency shall be responsible for complying with the requirements of this subchapter and related policies, procedures, standards and guidelines, including information security standards promulgated under section 11331 of Title 40, operational directives developed by the secretary under section 3553(b), and policies and procedures issued by the director. So this says the agency shall be responsible for doing those things.

THE COURT: So that establishes the mandatory duty. But my question is where then do I get the standards to determine from the statute whether or not they've complied with that statutory duty?

MR. PATTERSON: You would look at the directives that we are saying that they are not following, and that the

IG has set out in its report saying under FISMA they're required to do this.

For example, authorizations, which I think the decision there would be when they plug the system into the network without having it authorized, that, you know, somebody made the decision to do that. And so, that is a discrete decision.

THE COURT: So other than *Cobell* where the Court, in dicta, said this is not something that is reviewable under the APA, has any Court found it to be?

MR. PATTERSON: Not to my knowledge, no.

THE COURT: Okay. All right. Do you or does somebody else want to talk about the Little Tucker Act? But is there anything further you want to say about the APA or the Privacy Act before we go on to that?

MR. PATTERSON: Nothing else about the APA. But I'm prepared to talk about the Little Tucker Act, too, so --

THE COURT: Has any Court ever interpreted the SF-86 as a contract between the job applicant and OPM? And then I guess the question is: How do you answer their point that the statement that the Agency will do what it's legally obligated to do was consideration or bargained for in any way?

MR. PATTERSON: I'm not aware of any Court holding that one way or the other with respect to the SF-86, or at least not with respect to the language that we're pointing

to. And this case, though, is similar -- there's a case -- and I'm not sure this is cited in the briefs, but it's *Research Analysis and Development, Inc.*, 8 Claim Court 54, where the Court of Claims, before there was a CFC, the Court of Claims held that a person who wanted a contract with the government, there's this system for submitting unsolicited proposals to the government and there are regulations that say if you put a certain legend on it, we will keep your information confidential.

So, a contractor complied with that, the government sent them a letter that said pursuant to these regulations we will not disclose your information, and the government ended up disclosing it. And the Court of Claims held that was a contract and that was a breach of contract because the government was soliciting these proposals and they said -- pursuant to these regulations, saying we wouldn't disclose, they sent them a letter confirming, saying, yeah, we won't disclosure your stuff and then they disclosed it. And it's very similar to what happened here.

THE COURT: Well, is it different? I mean, there they made a promise, sort of voluntarily, here's this -- what we're going to do for you, if you give us this stuff. But in this situation what they're saying is -- it says on there the Privacy Act requires X, Y, and Z.

MR. PATTERSON: Right.

THE COURT: It's not, you know, if you do something that wouldn't otherwise be required, we're going to do something for you that wouldn't otherwise be required. They're just saying you should be aware that there's this statute out there. How does that create a contractual obligation?

MR. PATTERSON: Just to be clear, in that other case there was a regulation that said -- they weren't promising to go above and beyond the regulation. But here, what the consideration is, I think the government is saying we're going to bear the risk. They say we will protect your stuff from unauthorized disclosure. If it's disclosed, we're going to bear that risk. Under the Privacy Act we have to show intentional and willful. There are other requirements we have to meet. Here they're saying no, we will protect your information from disclosure. So if that information is disclosed, they've breached the contract, they've accepted the risks. So that is something beyond --

THE COURT: They're saying they're going to do it. But what's the -- the reason the person is filling out the form is because they want the government job or they want the security clearance. So to do that they must turn over their information. And the government is saying when you do that we're going to comply with the law. But that's not -- it's not in return for the promise that people give the

information. People give the information in return for being considered or as a necessary component of being considered for the job. How does this fit into any ordinary contract principle?

MR. PATTERSON: Well, presumably the government thinks it's valuable or they wouldn't put it on there, letting people know for sure we're going to protect your information. I mean, people, yes, they're required, if they want a security clearance or certain government job, to fill out that information, but people aren't required to work for the government. And the consideration is we're going to protect your information. And our submission is this goes beyond the Privacy Act because it doesn't have an intentional or willful requirement. It says we're going to protect your information, here are the disclosures that are allowed under the Privacy Act.

THE COURT: But they're saying that's not a offer, that's just a statement of what the law requires.

MR. PATTERSON: And it's the same thing as that Claims Court case that I cited you to, which is *Research Analysis and Development, Inc.*

THE COURT: When is this from?

MR. PATTERSON: 1985. And it's 8 Claims Court 54.

THE COURT: Obviously it's not binding.

MR. PATTERSON: Right. And I apologize, it's not

in the brief. I came across it studying for argument.

THE COURT: And I'm happy to look at it.

Well, let's go on to the next issue, which is Congress has created a specific remedial scheme for a statutory violation that includes money damages. We're all agreed that the Privacy Act includes money damages. So why didn't that displace the Little Tucker Act?

MR. PATTERSON: Well, I mean, I don't think that says that -- so in the Act, if we were just going based completely on the regulations and no statement in the form saying we're going to protect your information from disclosure, then, yeah, I think that would displace it because they would say, no, Congress has created this separate statutory regime.

But here it said the Agency is providing some extra degree of assurance and protection that your things --

THE COURT: It almost cites -- it quotes the Privacy Act, it cites the Privacy Act, it's got Privacy Act written all over it. It clearly doesn't offer anything other than the Privacy Act. So why wouldn't the Privacy Act, which says if that's violated you can get money --

MR. PATTERSON: That gets me back to the acceptance of the risk point, which is what, you know, the Supreme Court held in *Winstar* the government was doing there. But, it's that -- yes, under the Privacy Act you

have to show intentional and willful. Here they're lowering that by saying we're going to protect your information from an unlawful disclosure. If your information is disclosed unlawfully, we bear the risk.

THE COURT: Tell me the words on the SF-86 that says anything other than Privacy Act, Privacy Act, Privacy Act.

MR. PATTERSON: It says your information will be protected from unauthorized disclosure, and then it goes to the Privacy Act and says what's authorized. But I -- and, you know, you can disagree with the position here, but our position is that they've said that the effect of that promise is that if that information is disclosed in an unauthorized manner, that the government has effectively accepted the risk of that, similar to in *Winstar*, if, you know, the regulation that allowed the government -- the thrifts to treat capital in certain ways was changed, the government accepted the risk of that, and then that created a contract.

THE COURT: But you're still talking about whether there's a contract.

MR. PATTERSON: Yes.

THE COURT: I'm going to the second prong of their argument, which is that the Privacy Act displaces the Little Tucker Act, and that even if it doesn't, even if there is some kind of contract, doesn't it have to be a money-

mandating contract for the Tucker Act to apply? So where's the money-mandating aspect of this contract that you say was created by the offer to go -- to protect things?

MR. PATTERSON: Well, again, as the Court said in *Winstar*, as the federal circuit has said in many cases, there's a strong presumption that damages are available for a breach of contract. And there's -- and there's nothing that would indicate that damages were not intended for this. Damages are a completely appropriate remedy, as the Privacy Act remedy shows.

THE COURT: Well, if the Privacy Act remedy shows that, doesn't that just prove the point that the Privacy Act displaces the Tucker Act here?

MR. PATTERSON: Our submission is no because the government has gone beyond what was provided in the Privacy Act.

THE COURT: And they did that by introducing the discussion of the Privacy Act with the words, We will protect your data from unauthorized disclosure.

MR. PATTERSON: Yes.

THE COURT: Okay. All right. Is there anything else you want to tell me about the contract claim?

MR. PATTERSON: No.

THE COURT: Okay. I haven't heard from KeyPoint yet, but since they're next, maybe you want to address their

argument about why the state consumer protection statutes would apply in this context which doesn't involve consumer transactions or goods or services for sale.

MR. PATTERSON: My co-counsel is going to address KeyPoint, so --

THE COURT: All right. Did you get to tell me everything you wanted to tell me about all the other statutes?

MR. PATTERSON: Yes.

THE COURT: All right. Thank you.

MS. WOLFSON: Good morning again, Your Honor.

The state statutes that prohibit unlawful, deceptive trade practices are written very broadly and the focus is, is the defendant, sort of, in the usual course of business doing something that's unlawful? And that's precisely the situation here.

THE COURT: I mean, they don't just say did they do something unlawful in business. They're specific and they apply to consumer transactions, people selling goods and services. KeyPoint was contracting with the government to perform certain services for it. But how -- they didn't engage in any transaction with consumers here, and particularly not the plaintiffs. So I just don't understand how those statutes apply to this situation.

MS. WOLFSON: Well, we disagree with that. There is no privity agreement in these, what we call UDAP

statutes. KeyPoint was in the usual course of business being what it does, doing what it does, which is being a consumer reporting agency. And the plaintiffs in this case were consumers for the purpose of having their very sensitive personal information reviewed by that agency. And so the fact that OPM is sort of the middleman here to which our clients provided the information doesn't really change that analysis. It was --

THE COURT: Why do you say that what they do all day is to be a consumer reporting agency?

MS. WOLFSON: That's their business. They've admitted that in their privacy statements. They've conceded that point. They run background checks on people, in this case people who apply for positions with the OPM. And because of that license, they have obligations to protect that sensitive information under FCRA and other statutes. That's not a point of contention, that they're a consumer reporting agency.

THE COURT: All right.

MS. WOLFSON: And I just want to make a couple of other points. Under some statutes even business entities can be consumers. For example, under the Florida UDAP statutes and other statutes, there are cases that say they specifically apply to nonconsumers, under Illinois, New Mexico and Washington UDAP statutes.

THE COURT: I don't think the question is whether the plaintiffs are consumers as much as whether there was a consumer transaction on the KeyPoint side. They're not offering goods or services for sale to the plaintiffs.

MS. WOLFSON: I think in the ordinary course of business they were engaged in their usual business. We -- every time you apply for a job, every time you apply to rent an apartment background checks are run, credit reports are run. And just because you may not know who exactly is doing that, doesn't mean there's not a consumer transaction there and certain duties and obligations.

THE COURT: All right. Do you want to address any of their other arguments? That was the one that I particularly wanted to point you to.

MS. WOLFSON: Under the state statutes against KeyPoint, so they make a big deal about Rule 9, which we do comply with. And we set out in our brief the paragraphs that talk about, you know, specifically how there was deceptive acts here. But an important point is that a lot of these statutes also have the unfair and unlawful prongs of the statutes, and Rule 9 does not apply to those.

So the bulk of our contention is that they failed to implement safeguards with regard to their cybersecurity and that was unlawful and unfair and Rule 9 does not apply to those allegations.

Also, under the --

THE COURT: What is the allegation that lays out what was deceptive, as opposed to inadequate or deficient?

MS. WOLFSON: Well, mainly what was deceptive is that they did not inform class members that their privacy cybersecurity safeguards were inadequate, and that's an omission type of deception. And we contend that consumer behavior would have changed had they known that.

For example, they may have applied, you know, for identity -- credit identity services, identity theft protection services, sorry, sooner. They may have chosen to place credit freezes if they knew that their information wasn't as protected as it should have been.

THE COURT: Is there anyone -- I think we talked about this earlier, at the last hearing, I believe the plaintiff said that none of the plaintiffs in this case have a claim based on the KeyPoint breach. They're all based on the OPM breach. So how was the failure to inform someone that their privacy was inadequately protected, how did that cause or lead to a single one of the injuries being alleged in this case?

MS. WOLFSON: So we allege that KeyPoint handed over login credentials to unauthorized people and because of that the consequence was that class members' information, both from the OPM database and the KeyPoint database, was

breached. This is --

THE COURT: Well, that's your negligence claim. But that's -- how does that get to your deceptive -- if no one who gave their information to KeyPoint is suing because that information was unlawfully disclosed or unlawfully deficiently protected, then what difference does it make if they told people their protections were adequate or inadequate?

MS. WOLFSON: Because class members would have acted differently with regard to giving their information to OPM if they knew that as part of that transaction KeyPoint was going to run their background checks and they did not have sufficient safeguards to protect their privacy.

THE COURT: Right. But those aren't the people that they're saying were part of the breach. They're not saying that information leaked out of KeyPoint to the hackers. The last time I was specifically told on the record that the 22.1 million people we are talking about are the people whose data was scooped up out of OPM by the hackers.

MS. WOLFSON: As a result of KeyPoint's inadequacies, including handing over the login credentials into the OPM system.

THE COURT: Right. But, whether or not KeyPoint did a good job maintaining its login credentials and is, therefore, liable, whether you've stated a claim that they

were negligent and that negligence was a link in the chain to the breach, that's a different claim than saying when people gave them data, they relied on this deceptive omission about the inadequacy of their procedures. That isn't tied to a single allegation of a single plaintiff, as I understand it. So what does that have to do with anything?

MS. WOLFSON: Well, so, I'm not sure what the question is. I think that, if anything --

THE COURT: My question is: You are suing them for deceptive consumer -- deceptive conduct in terms of how they deal with consumers, basically lying to consumers. And the consumers, you say, are the people who gave them -- them -- their data to be analyzed. And the lie upon which they relied to their detriment that you say you set out with sufficient specificity under Rule 9, is that they failed to say, by the way, we're not going to take care of this very well.

MS. WOLFSON: I think I understand the issue. The link -- the chain of events here is that the consumers give the information to OPM, who then forwards their information to KeyPoint to conduct --

THE COURT: That's not the information that went missing here. It was not the KeyPoint breach.

MS. WOLFSON: But the information flows both ways. So OPM gives information to KeyPoint, KeyPoint enhances it

with their background checks and then sends it back to OPM. And we do allege that that -- OPM's entire database, which includes information provided by KeyPoint, is what was breached as a result --

THE COURT: Because it was infected when it came back? That's not in the complaint.

MS. WOLFSON: No, because KeyPoint provided the hackers the login credentials to get --

THE COURT: It doesn't say that in the complaint. It says the hackers hacked with a stolen -- stolen is your word -- KeyPoint credential. And then you argue later, in paragraphs 400 or something, in the negligence count, that they are negligent because they didn't do a good enough job keeping a handle on who had their login credentials or not. And they argue that those are all too conclusory. We're not talking about that right now. I can figure out without argument whether it's conclusory or not by reading it.

But I'm trying to figure out where the deceptive consumer practices stuff ties back to a single plaintiff.

And someone wants to say something.

MR. ELIAS: Right. Jordan Elias, Your Honor. If I might. Can we consider an alternate scenario perhaps, where KeyPoint did in fact disclose the inadequacies of its security, and let's consider a plaintiff or a class member who had provided his or her sensitive private information to

the government, how would that disclosure by KeyPoint, whose's recognized as the government's background check contractor, have affected that individual's actions --

THE COURT: Is it the government's background check contractor for every single background check?

MR. ELIAS: I believe at a certain point they became such, around 2014.

THE COURT: Is there anything about the fact that they were doing the actual background checks and that that had something to do with this breach that's in your complaint anywhere? I don't need to consider hypotheticals, I only need to consider what's on the face of the complaint, and the face of the complaint says 22.1 million people's data went missing because of a sophisticated and malicious hack of the OPM database in which every single plaintiff's data resided and from which every single plaintiff's data departed.

MR. ELIAS: Correct.

THE COURT: And that breach was occasioned by the fact that the hacker had a KeyPoint credential that it stole.

MR. ELIAS: As a result of KeyPoint's unreasonably deficient security, of which many elements we have itemized.

THE COURT: And that's your negligence count, and which either rises and falls, first of all, with the government contract immunity issue that we talked about last

time. And if it gets past that, then it rises and falls with the adequacy of the negligence allegations for 12(b)(6) purposes where I have to resolve all inferences in your favor, but I don't have to accept your conclusions, and we know all that. So I'm not talking about negligence right now, which is what you're talking about.

I want to know whether there's any causal connection between the alleged deceptive conduct -- we're not going to take good enough care of this -- and the plaintiffs' claims, which is that OPM didn't take good enough care of this. Nowhere in the complaint is it alleged that the stuff got hacked when it was sitting in KeyPoint's database. Your whole argument is that the government didn't comply with FISMA, the government didn't comply with the Privacy Act, the inspector general told the OPM that its security wasn't good enough and somebody breached it. Isn't that your case?

MR. ELIAS: Well, that's part of our case. That's mainly the case against the government. But --

THE COURT: Tell me where your case against KeyPoint says people got into your system and stole people's private information from your system. That's not in there.

MR. ELIAS: Well, we do, you know, allege a KeyPoint class of people whose information was taken from KeyPoint in the KeyPoint breach that happened in December of

2013. Now, it's true that no individual plaintiff alleges that they gave KeyPoint their information directly, maybe that's because the investigators didn't identify themselves as being with KeyPoint.

But the key -- still, the link is still the same as for the negligence count, Your Honor. It's that the unreasonably deficient security of KeyPoint is precisely what allowed the security credentials to be stolen and, in turn, used as the proximate cause of the overall breach.

And let's consider what -- how that disclosure from KeyPoint of its inadequacies would have affected the behavior of someone who had given their information to the government because that is the analysis of the materiality --

THE COURT: And when someone gives their information to the government --

MR. ELIAS: That's the analysis of materiality, would it have affected the person's behavior in an important way in a transaction?

THE COURT: How does anyone know, when they're giving information to the government, that it's going anywhere other than the government?

MR. ELIAS: Well, if KeyPoint had disclosed that it needed to patch up its systems and they weren't good enough --

THE COURT: To whom?

MR. ELIAS: If they had announced it publicly, if they told people during the background checks, that likely would have caused people to go out and do things, like John Doe II did, which is to buy $329 annual credit protection.

THE COURT: But do the applicants interact with KeyPoint during their background checks?

MR. ELIAS: That's my understanding, that they do interviews. I don't really know.

THE COURT: Okay.

MS. WOLFSON: That goes back --

THE COURT: I'm confused. You mentioned the KeyPoint class and the 2013 data breach. I thought last time I was told that every plaintiff in this case is suing because of the OPM data breaches. So was that a misstatement? There is a separate subset of plaintiffs that is suing based on the KeyPoint data breach, as opposed to the KeyPoint failure to keep ahold of its credentials?

MR. ELIAS: Well, I think what we said is that we don't have an allegation that any plaintiff received notice of being subject to that smaller KeyPoint breach -- smaller being 48,000 people.

THE COURT: So there's no one in the class that you know of?

MR. ELIAS: Well, that's a different issue. You

know, there may be people in the class whose information was in both databases. We wouldn't be able to know until discovery.

THE COURT: All right. Is there anything else you want to say about the KeyPoint motion to dismiss the state and common law claims?

MS. WOLFSON: Yes. I would like to address the FCRA cause of action.

THE COURT: Okay.

MS. WOLFSON: So, KeyPoint's entire argument that you should dismiss the FCRA cause of action is they say they could not furnish the information under FCRA because there was a theft. And they make the analogy that if someone breaks into your car, you could hardly be said to be furnishing your stereo to a thief. But that's not what our complaint alleges. Our complaint actually alleges that KeyPoint, in essence, gave the keys to the car, which is the login credentials to the thiefs. And so this premise that when you have a theft you could not furnish it, the information under FCRA, is just simply not correct.

THE COURT: But again, are you talking about the theft in 2013 from their database or are you saying that they furnished the data that was stolen from the OPM in 2014-15.

MS. WOLFSON: Well --

THE COURT: How could they furnish that?

MS. WOLFSON: They furnished, you know, the keys to the castle. And to clarify, there isn't -- it isn't a fact that there is a, you know, discrete OPM database and a discrete KeyPoint database. What's happening here is there's a network over the internet, which is essentially a network that's a publishing and open to the world but for the safeguards that both OPM and KeyPoint are supposed to implement.

THE COURT: I don't think that's how the complaint reads. The complaint reads that a hacker hacked OPM because it had a KeyPoint credential to get into OPM's data. It doesn't say that the hackers scooped out of both, that they used KeyPoint's access to get into OPM's data. That's the whole complaint. Where is what you just said in the complaint?

MS. WOLFSON: Well, I think we do allege that OPM was furnishing information to KeyPoint and vice versa. And if we need to do a better job to that, then you should give us leave to amend to do so. But I think the facts do contemplate that there's a communication, electronic system between the two over the internet and but for the safeguards that KeyPoint and OPM should have implemented, it's open to unauthorized people.

THE COURT: All right. Well, I'm going to read

the complaint more carefully, but I'm not seeing what you say that's in there in there.

MR. ELIAS: Paragraph 76.

THE COURT: All right. So they're connected, but -- well, I'll look at it. But the whole theory, it seems to me, is that what got hacked, it wasn't that they -- well, the whole case is about OPM's protection of what it had.

MS. WOLFSON: Which was part of this communication network. And KeyPoint, as well as OPM, had an obligation to keep that secure. But going back to this concept that if you have theft you can't have furnishing, which is really the buttress of KeyPoint's argument, I'm going to point you to a case called *Andrews versus TRW*, 225 F.3d 1063, it's a Ninth Circuit case from 2000. And there an unauthorized person received a consumer report from TRW and used it to commit financial fraud. That was a motion for summary judgment that was overturned, including a claim for punitive damages. And the Court said that it's a factual inquiry for the jury to see whether TRW implemented the correct safeguards to make sure that the sensitive information didn't get into the wrong people's hands.

So, that's for the proposition that you can in fact have theft and have a furnishing under the FCRA. Similarly, *Harrington versus Choicepoint*, which is at 2005

C.D.Cal., stands for that proposition. And it's interesting how strikingly similar those allegations are to those in our complaint.

THE COURT: But, the theft has to be from the repository of the data. I mean, here the theft was from TRW. And what you're saying is the fact that the theft was from OPM, the fact that it was facilitated by KeyPoint credentials is enough to make it analogous to this situation.

MS. WOLFSON: Yes, it is. Because the focus is what are KeyPoint's duties under the FCRA, and that is to protect consumer information, both that it collects and that it has access to in the OPM database.

THE COURT: Well, if, with respect to the Privacy Act claim, the plaintiffs have not conceded, but certainly said with respect to whether you've got willful disclosure, it really -- we're not pushing that, what we're pushing is willful failure to maintain adequate safeguards because when Judge Robertson distinguished a breach from a failure to maintain safeguards, that there could be a willful failure to maintain safeguards, but not a willful disclosure, why didn't that same -- why doesn't furnishing kind of rise or fall the same way disclosure does, that failure to protect against a malicious crime is somehow different than furnishing or disclosing, which is an active verb.

MS. WOLFSON: Well, because if you look at -- if

you apply statutory construction rules to the FCRA, under the plain meaning of furnish, it does encompass, you know, more passive acts to be the source of. An example I like to prove our point is fish can furnish protein to its predators. And so really, when you're talking about cybersecurity --

THE COURT: Fish?

MS. WOLFSON: Well, the point is that --

THE COURT: I want to make sure I understood what you just said. Okay.

MS. WOLFSON: Fish, yes. You can be an involuntary source of something that you are obligated to protect, not just through some kind of act of volitional transmission, but through failure to safeguard. And we do -- I think the word "furnish" encompasses that definition and the protection of --

THE COURT: So they don't merge for the Privacy Act but they merge for purposes of the FCRA?

MS. WOLFSON: When you say they merge, they merge in the sense that, yes, you can have a more passive to be a source of something versus a volitional, you know, direct, here you go, here's the information.

THE COURT: Is there a requirement of willfulness or intent in the furnishing under the FCRA?

MS. WOLFSON: There is for statutory damages, but

not for other claims.

And I want to distinguish the cases that defendants -- that KeyPoint cites for the proposition that, well, if you have a data breach you just don't have furnishing. *Willingham versus Global Payments*, *Holmes versus Countywide*, and *Dolmage versus Combined Insurance Company of America*. All those cases first held that the defendants there were not consumer reporting agencies. And then they made very short shrift of the definition of furnishing. And we don't think that those are as important as the cases we cited, *Andrews versus TRW*.

And, you know, while defendants don't provide a definition of furnish, implicit in this argument is exactly what you pointed out, which is there has to be some sort of voluntary, volitional, intentional act. And that's just not the case. If you look at the plain meaning of the word, if you look at FCRA purpose, which is codified right there in the statute under 15 U.S.C. 1681b, which is to require consumer reporting agencies to adopt reasonable procedures to ensure confidentiality of consumer reports.

Guimond versus Trans Union, a Ninth Circuit Case, as well as *Cortez*, a case that KeyPoint cites, instruct us that FCRA is a consumer-oriented statute and that it should be construed very liberally to protect consumer privacy.

And also, what the FTC -- how the FTC has enforced

FCRA should have at least *Skidmore* type of weight here, and they've had no problem applying the FCRA to data breach context. And we've given you several examples of those in our brief. Commissioner Brill has also stated that the FCRA requires consumer reporting agencies to take reasonable measures to ensure consumer reports are provided to authorized entities only.

So, we don't think that under the statutory construction principles you do need to have this volitional, intentional act. But even if you do decide to adopt that definition, we think we allege it because, as I mentioned earlier, we think the entire setup of this furnishing database, an electronic conduit over the internet between OPM and KeyPoint is a volitional act of furnishing, but for the safeguards that they were supposed to implement to make sure it doesn't get into the wrong hands.

And secondly, the furnishing of the login credential is also, you know, a volitional act to the extent that you want to apply that narrow definition.

And the final point on FCRA is that, you know, this is a very fact-specific inquiry, if we're going to focus on what does furnishing mean, how much intent, how much, you know, active act does it require? That's a fact specific inquiry and we would respectfully request that you make those decisions on a full evidentiary record.

THE COURT: All right. I think, yes, a lot of these are factual issues and we're not talking about the immunity issues, it's a question whether I reach them. Certainly with respect to negligence, it's a factual issue.

All right. Is there anything further that you wanted to emphasize right now?

MS. WOLFSON: I'm prepared to discuss the state data breach loss. I don't have anything that I want to emphasize, but if you have questions about that, I'm prepared to address them.

THE COURT: I don't have any questions right now on that. All right. Thank you.

MS. WOLFSON: Thank you.

THE COURT: All right. Let's go on to KeyPoint, then we'll finish up with NTEU again. To some extent you were arguing last time that the allegations were insufficient to establish causation because they -- causation for standing purposes because they didn't allege anything specific that the contractor did that was negligent that led to the data breach. And is that a standing issue or is that really a 12(b)(6) issue? I mean, isn't this when we should be talking about that, or did that go -- do you think it was a standing issue?

MR. MENDRO: I think there's both, Your Honor. Certainly it's 12(b)(6) issue, there's no question about that.

But the point that we were making last week with regard to standing is that all of the steps that need to be taken to get from the plaintiffs to standing with respect to OPM or are attenuated by one more step with regard to KeyPoint. Because as Your Honor pointed out, although the plaintiffs allege that a KeyPoint credential was used in order to access OPM, there isn't any allegation that that credential was actually taken from KeyPoint. In fact, the allegations in the complaint don't necessarily support that inference.

There's allegations that before the KeyPoint data breach, which of course was not the source of the exposure of any of the named plaintiffs' information, but before that time there was an alleged breach into OPM's system, an earlier OPM breach which allegedly exposed the entire data blueprint, security blueprint for the OPM system, including credentials.

So there really is no allegation that even though a KeyPoint credential was used, that it was taken from KeyPoint, nor is there any reason to infer from the allegations that KeyPoint was negligent even in that respect. And that's why we're saying that all of the steps that it takes to get to standing for the government are attenuated by one more with regard to KeyPoint.

The same arguments bear heavily on our 12(b)(6)

motion, especially with regard to negligence.

THE COURT: Wouldn't the allegations concerning negligence just -- they didn't do a good enough job maintaining the security of their access codes and it was one of their access codes that was the keys to the kingdom, as the plaintiffs pointed out. If we're just talking about inferences and pleadings and resolving inferences in favor of the plaintiffs, with respect to the negligence count, isn't that enough?

MR. MENDRO: Well, let me point out what the complaint doesn't plead because I think that will explain why there isn't enough. The -- this actually answers, I think, every single one of the counts in the complaint. It's particularly pertinent to negligence. But I think the absence of these allegations address all of the counts in the complaint and render some of them quite nonsensical.

But the plaintiffs didn't plead any plausible connection between them and KeyPoint at all. We've now said many times at this hearing and the last, that there's no allegation that any plaintiff's data was lost in the KeyPoint data breach. But it's much worse than that, Your Honor. There's no allegation that any of the plaintiffs actually were subject to a background check by KeyPoint at all. There's no allegation that any of the plaintiffs was interviewed by KeyPoint. There's no allegation that any of

the plaintiffs actually provided their personal information to KeyPoint. There's no allegation that KeyPoint obtained any of the plaintiffs' personal information in any other fashion. And when you combine that with the acknowledgment that there isn't any allegation that the plaintiffs' information was lost in the KeyPoint data beach, what you quickly find is that none of these counts state anything but a conclusionary assertion of liability, which is not sufficient to state a claim.

THE COURT: Well, I mean, we were having that lengthy discussion about all of the consumer claims, how does the failure to disclose that you don't have adequate security relate to a situation that you just described, where nobody is saying that that's where people's background checks were being done or that's where the data escaped from. But, when they argue in the paragraphs that they kept pointing to last time for causation purposes that it wasn't KeyPoint's failure to protect the integrity of plaintiffs' data, it was KeyPoint's failure to protect the integrity of its access codes, which is where it fell down on the job, why doesn't that state a claim for negligence?

MR. MENDRO: Well, for two reasons. Because, number one, when there's an intervening criminal act as alleged here, there is a heightened requirement for there to be causation in order to state a claim for negligence. And

what that heightened requirement entails is either an allegation that there's a relationship, a fiduciary type relationship, or some kind of connection between the plaintiffs and the defendant, or an allegation of control between the defendant and the criminal -- the intervening criminal actor. And we don't have that here because, as I just --

THE COURT: It is the criminal act that you're protecting against, that is the foreseeable thing, harm that you're protecting against in the first place, it's -- that's the harm. Isn't it different, the foreseeability standard and the heightened causation, when you're talking about not the kind of crime that can happen anywhere on the street. Perhaps KeyPoint didn't have the duty to protect people from an armed robbery, but to protect them from the only kind of crime that can only happen to people by virtue of attacking KeyPoint, that's not subject to the heightened causation, is it?

MR. MENDRO: It is, Your Honor. And once you take into consideration that none of the plaintiffs' information was lost from the KeyPoint database, this case begins to look very much like the *Romero* case that was decided by Justice Scalia when he sat on the D.C. Circuit. That is a case where the criminal wrongdoers broke into the NRA, stole something from the NRA and then went out and committed crimes with it.

And that's very analogous to what the allegations are here. Here the plaintiffs are saying that somebody broke into KeyPoint's facility, stole something from KeyPoint, and then went someplace else to do something wrong with what they stole.

Now, here's one difference that I would point out between this case and *Romero*. In the *Romero* case there's at least the allegation that it was the NRA's stolen gun that was used for the crime, and that it was stolen from the NRA. Here, we don't even know if the KeyPoint credential was stolen from KeyPoint. So this is a *Romero* case, but I think an even weaker one.

The other point I want to reemphasize, I won't -- certainly won't repeat the governmental immunity, derivative immunity arguments that we discussed when we were here last. But every single one of plaintiffs' claims have to be dismissed due to KeyPoint's immunity unless they can allege a violation of some requirement that was clearly established. And the complaint doesn't plead that there was anything that KeyPoint was required to do to meet the duty of care that it failed to do. There's only bald assertions of not doing something good enough, not doing something adequate.

But there are no assertions that it was established, at the time of these events, that in order to

meet the duty of care KeyPoint had to do something that it failed to do. And without that type of allegation the immunity would foreclose these arguments, even if the other 12(b)(6) issues didn't.

THE COURT: All right. I don't have any more questions for you. You're welcome to highlight or add anything you wanted to highlight or add in light of the arguments that you heard about furnishing or the other issues about being a reporting agency.

I mean, what she's saying is if they are a consumer reporting agency, which you agree, you fall within that, then what they did was a consumer transaction essentially. And you've argued that the consumer protection statutes don't apply because these were not consumer transactions with goods or services for sale. So what's your response to her argument?

MR. MENDRO: The answer, Your Honor, is that there is no consumer relationship. There is no relationship. There's no allegation that anybody, but one plaintiff who apparently worked at KeyPoint, even ever heard the word KeyPoint. So there isn't a consumer connection, or any connection. There's no nexus to any consumer transaction. Nothing in this case has to do with a consumer transaction. These are applications for jobs. So I would say that those statutes are very square pegs in very round holes and don't

apply.

With regard to --

THE COURT: But if someone knocked on their door and rang their bell and they said here's my information, please do a background check on me, would that be a consumer transaction?

MR. MENDRO: Conceivably, if somebody said I'm going to pay you in exchange for the service of conducting a background check on me, I think that might be a consumer transaction. That would be a different case than this case.

And very briefly on the Fair Credit Reporting Act claim, the FCRA claim, I'm not in a position to address the TRA case -- or, *TRW* case, rather. I don't believe that case was cited in the briefs.

The *Harrington* case that was cited in the briefs and mentioned just a few moments ago is a completely different context and I don't believe that the Court there actually analyzed the meaning of the word furnish.

Plaintiffs counsel did mentioned that we've cited three cases, *Dolmage*, *Willingham*, and *Holmes*, all of which do interpret the word furnish to conclude that it means active transmission. That's not necessarily the same thing as intent, which I think is what was being said, but involves active transmission and, of course, that comports entirely with the common understanding of the word furnish.

The only other authorities that the plaintiffs cite are three unadjudicated FTC complaints, all in the context of litigation, which are entitled to absolutely no deference at all under law, and a stylized quotation to Winston Churchill concerning the medieval outlook. So those are not authorities that I think could conceivably justify interpreting furnish to mean being stolen from.

So if the Court doesn't have any other questions --

THE COURT: That's it.

MR. MENDRO: Thank you, Your Honor.

THE COURT: All right. Thank you.

Last but not least, counsel for NTEU.

Your standing argument last time was predicated pretty much exclusively on the fact that we were talking about a constitutional violation. So now we're finally talking about the merits and I want to know if any court has actually recognized a constitutional right to informational privacy in connection with a criminal data breach. In other words, even if your private information has some protection, which some cases have suggested it does, how did a criminal theft of that information implicate your constitutional rights?

You have found a law review article in which the author suggests that the right to privacy points us in that direction. And that's -- that's nice, but that's usually

not enough, since you could probably find a law review article that points in the opposite direction if I looked for it. So, where do I find the precedent that takes me that far?

You seem to be building your cases on a constitutional level of privacy protection from cases that talked about privacy but then said there wasn't a constitutional violation, or cases where the government is taking your information in the Fourth Amendment context. So, what have you got?

MR. SHAH: Your Honor, to answer your first question, there has not been a constitutional right to informational privacy violation found in a data breach case.

Here, our theory is based upon existing precedent, applying the right in the post disclosure context. Our legal theory is predicated primarily on the cases discussed in pages 31 to 38 of our brief, where courts of appeal have built upon the initial analysis of the right and the Supreme Court jurisprudence, also discussed in our brief. And I'll gladly sort of take you through those cases and why we think they have application here in this context.

THE COURT: I read your brief, and I can read the cases and I've read some of the cases, so I would actually -- if there's something you want to do to synthesize it, I would appreciate that but, you know, I think you should

trust my ability to actually read what you gave me. And I don't mean that -- I'm not trying to be insulting. I really have dug into all of this because it's very, very interesting and it's very important.

But, you've talked a lot about disclosure. And if there was some active governmental act of saying I'm giving away somebody's private stuff, even if that's the next logical step for where the law should go after saying the government can't unlawfully collect somebody's private stuff, since what everybody agrees what we're really talking about is the failure to adequately protect the private stuff, that's one step more even than all the cases you point to which have an individual interest in avoiding a disclosure of private matters. How do we get to failure to safeguard, which is I think where you have to go to get a constitutional right here.

MR. SHAH: Your Honor, here's what the disclosure cases show: They do show that the constitutional right itself creates an affirmative obligation that in the very least requires the government not to disclose information that it collects on the promise of confidentiality, inherently personal information. And our view is that if the right is violated, where the government takes inherently personal information on a promise of confidentiality and then turns around and gives that information to a third

party that shouldn't have access to it, it must logically follow that if the government can't simply hand that information over to somebody else, it, likewise can't, in effect, leave that information in a room with all the doors and windows open.

THE COURT: Maybe statutorily, but if you're talking about the constitution and shocking the conscience and substantive due process and liberty and property interests, aren't we talking about something different? Doesn't it have to be more egregious than just not doing a good enough job to protect it? Or even really not doing a good enough job to constitutionally protect it?

MR. SHAH: What we allege here is that OPM's reckless or deliberate indifference in safeguarding information, indifference that facilitated the hackings that occurred and indifference that continues, and continues to put our members at risk of additional breaches, that indifference is what raises to the level of a constitutional violation.

And Your Honor is correct that we do base this theory on language in *DeShaney* which the government referenced in its opening, as well as a scholarship analyzing a constitutional right. At its core what *DeShaney* says and what D.C. Circuit precedent, extrapolating on *DeShaney* indicates, is that where -- for example, where the

government has physical custody over an individual and that individual is helpless in certain ways, there is an affirmative obligation on the part of the government that can be violated and violate the Fifth Amendment due process clause.

Here our theory is that the government here, it has compelled our members to disclose inherently personal information to it. To get and keep their jobs they had to give this information up. And the government, in turn, has full control over what it does with that information and whether it protects or does not protect that information.

That is a very similar situation where the government has full custody and control and, therefore, its reckless indifference in safeguarding that information is sufficient to rise to a constitutional level.

So that's why we believe that it isn't inconsistent with Fifth Amendment due process clause jurisprudence to impute upon the government here where it is required information to be disclosed and it's promised to protect it, it is not in conflict with existing jurisprudence in the Fifth Amendment context to impute upon it an affirmative obligation to safeguard that information.

We believe that is in keeping with the Court of Appeals precedent indicating there is an affirmative obligation to not deliberately turn over. We believe that

it's an analogous thing to say, okay, if you can't turn it over, you can't leave it so insufficiently guarded that somebody can just walk in and take it.

THE COURT: All right.

MR. SHAH: I just want to make clear the government's position is that under the constitutional rights itself it has no obligation whatsoever to protect information in any way at all. And this view of the constitutional right is so hollow, it's so narrow that although it requires a justification by the government to collect information, the right ends right there and provides no protection going forward. And that --

THE COURT: Is even the right -- I mean, there's case law that suggests that the Court should find that there is a right. But is even the right to informational privacy itself established as a matter of binding precedent for this Court?

MR. SHAH: Not as a matter of binding precedent. The Supreme Court has only assumed the existence of the right. The D.C. Circuit has, in different decisions in dicta on the one hand acknowledged the right, on the other hand expressed some doubts on the right. The D.C. Circuit has not had occasion to give sufficient guidance to this Court as to whether the right exists. But as we noted in our brief, four judges on this court have analyzed claims

based upon the right, including two judges who did so even after the D.C. Circuit, in *AFGE v. HUD*, expressed some doubt to its existence.

THE COURT: Weren't all those cases collection cases?

MR. SHAH: They were. That was the factual posture of those cases.

THE COURT: All right. All right.

MR. SHAH: And just one last point, Your Honor. I want to be clear here that we are not arguing that a simple violation of FISMA is a constitutional violation; that's not what we're tying to do. It is the reckless indifference of OPM, and indifference that is described in detail in our complaint and in reports of the inspector general, it is that reckless indifference that we allege rose first to a constitutional level. And I would certainly encourage Your Honor to look at paragraph 88 of our complaint.

THE COURT: I'm sorry. 88?

MR. SHAH: 88, in which OPM's inspector general -- and this is months after the breaches occurred, he says this: For many years we've reported on critical weaknesses in OPM's ability to manage its IT environment and warned that it was at increased risk of a data breach. Our recommendations appear to garner little attention, as the same findings were repeated year after year. And the OIG

goes on to say that there's an overall lack of compliance that seems to permeate the Agency's IT security and that because of that general atmosphere -- and this is our words, not his -- but that general atmosphere of indifference, the IG remains very concerned that the agency's systems will not be protected against another attack.

That, we believe, illustrates OPM's reckless or deliberate indifference in safeguarding our members' inherently personal information. And that's the core of our legal theory, not a simple violation of FISMA.

THE COURT: Thank you. All right.

Well, I'm not sure really that I have more questions for OPM, unless there is something you're dying to say in response to what you heard. I don't want to shut you down, but I think I know your response to most of what you heard, or can anticipate it.

MR. PATTERSON: Two very quick points.

THE COURT: All right.

MR. PATTERSON: One point on the preclusion argument. I did want to point out that Judge Collyer did note in a footnote just last week that the Privacy Act does preclude the APA. Just wanted to highlight that for the Court. We noticed up the case.

Also, with respect to preclusion, it would make no sense at all for Congress to have created the scheme that it

created if the plaintiffs were correct. There would be absolutely no need to lay out injunctive remedies if all along you could just get across-the-board injunctions for Privacy Act violations.

On the discrete agency action, just a general point, when you're talking about information security rules, it's important to remember that today's standard may not be tomorrow's standard. It's constantly evolving. It changes all the time, which is, as a general matter, supports our theory that you cannot challenge a discrete agency action when you're talking about the standard that's constantly changing from one day to the next. I just wanted to point that out. That's it.

THE COURT: Okay. Thank you. Thank you, everyone. I think I now have the entirety of all of the motions to dismiss under advisement. I have a lot to think about. And I appreciate the quality of all of the arguments.

Mr. Girard, did you want to say something? You looked like you did.

MR. GIRARD: I am not purporting to open up a broader discussion. We had asked in our opposition to the motion to dismiss for leave to amend, if there are points that the Court deems to be amendable. We would reiterate that request. Thank you.

THE COURT: All right. It is now a matter of

record that you've made that request. Thank you very much, everyone.

* * *

CERTIFICATE OF OFFICIAL COURT REPORTER

I, JANICE DICKMAN, do hereby certify that the above and foregoing constitutes a true and accurate transcript of my stenograph notes and is a full, true and complete transcript of the proceedings to the best of my ability.

Dated this 11th day of November, 2016.

/s/_____

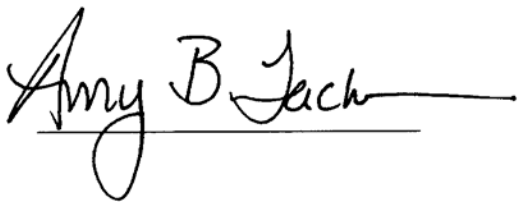
Janice E. Dickman, CRR, RMR
Official Court Reporter
Room 6523
333 Constitution Avenue NW
Washington, D.C. 20001

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN RE: U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION	Misc. Action No. 15-1394 (ABJ) MDL Docket No. 2664
This Document Relates To: ALL CASES	

ORDER

Pursuant to Fed. R. Civ. P. 58 and for the reasons stated in the accompanying Memorandum Opinion, it is hereby ORDERED that Defendant KeyPoint Government Solutions, Inc.'s Motion to Dismiss Plaintiffs' Consolidated Amended Complaint [Dkt. # 70], Federal Defendant's Motion to Dismiss the Consolidated Amended Complaint [Dkt. # 72], and Federal Defendant's Motion to Dismiss the NTEU Plaintiffs' Amended Complaint [Dkt. # 81] are GRANTED and the above-captioned multidistrict litigation is DISMISSED.



AMY BERMAN JACKSON
United States District Judge

DATE: September 19, 2017

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN RE: U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION	Misc. Action No. 15-1394 (ABJ) MDL Docket No. 2664
This Document Relates To:	
ALL CASES	

MEMORANDUM OPINION

INTRODUCTION

In June of 2015, millions of unsuspecting federal employees sat down at their computers, opened up their email, and received some very disconcerting news.

> I am writing to inform you that the U.S. Office of Personnel Management (OPM) recently became aware of a cybersecurity incident affecting its systems and data that may have exposed your personal information.

Over time, OPM revealed that data breaches at the agency and at one of its contractors affected more than twenty-one million people, and that the stolen information included such sensitive data as names, birthdates, current and former addresses, and Social Security numbers. After those announcements, a number of plaintiffs filed separate lawsuits in courts across the country, and they were consolidated into two complaints in the multidistrict action assigned to this Court.

The first complaint is a class action lawsuit filed by thirty-eight individuals and a union, the American Federation of Government Employees ("AFGE"). *See* Consolidated Amended Complaint [Dkt. # 63] ("CAC"). Plaintiffs allege that the breaches resulted from gross negligence on the part of officials entrusted with the responsibility of protecting the private details that job seekers submit to OPM in connection with the background investigations they are required to

undergo. They have sued on behalf of the 21.5 million current and former federal employees, job applicants, contractors, and relatives whose information was compromised, and they seek statutory damages under the Privacy Act, contract damages under the Little Tucker Act, and declaratory and injunctive relief under the Administrative Procedure Act. These plaintiffs have also sued KeyPoint Government Solutions, a government contractor that performed background investigations for OPM. KeyPoint's computer systems were also breached, and plaintiffs seek damages from the company under multiple federal and state statutory and common law theories. Defendants have moved to dismiss the entire case on the grounds that plaintiffs lack standing to bring it, the claims are barred by sovereign immunity, and the factual allegations are not sufficient to state valid claims under any of the statutes or common law theories plaintiffs have invoked.

The second complaint before the Court was filed by three individuals and the National Treasury Employees Union ("NTEU"). Am. Compl. [Dkt. # 75] ("NTEU Compl."). These plaintiffs sued the OPM Acting Director only, and they claim that their constitutional right to informational privacy was violated. Defendant has moved to dismiss that case as well, on both standing grounds and the basis that the plaintiffs have failed to allege a constitutional violation that is recognized by the courts.

The OPM breaches have been the subject of considerable public interest and multiple Congressional hearings and reports. The fact that the breaches occurred is not disputed, and the identities of the individuals whose information was compromised are known. There is no doubt that something bad happened, and many people are understandably chagrined and concerned. In these lawsuits, plaintiffs seek to demonstrate that the agency's failures were willful – that the defendants were on notice that hackers regularly targeted their systems, but they failed to design

and maintain adequate safeguards. Plaintiffs also contend that their sensitive information remains subject to a continuing risk of additional exposure due to an ongoing failure to secure it.

This opinion will not get into the merits of those contentions. At this stage of the proceedings, the Court is required to accept all of plaintiffs' factual assertions as true, and nothing that follows should be read as any indication of the Court's view of the strength of plaintiffs' troubling allegations.

Before the parties can explore the facts, though, the Court is required to answer a foundational question: whether plaintiffs have set forth a cause of action that a court has the power to hear. The judiciary does not operate as a freestanding advisory board that can opine about the conduct of the executive branch as a general matter or oversee how it manages its internal operations. The Court's authority is derived from Article III of the U.S. Constitution, and a federal court may only consider live cases or controversies based on events that caused actual injuries or created real threats of imminent harm to the particular individuals who brought the case. In other words, before a court may proceed to the merits of any claim, the plaintiffs must demonstrate that they have constitutional "standing" to sue. Also, a court may not entertain an action against the United States if the government has not expressly waived its sovereign immunity, that is, unless it has given its consent to be sued in that particular situation. And once a plaintiff overcomes those hurdles, he or she must state a valid legal claim.

This case implicates the constitutional limits on the Court's jurisdiction imposed by both the standing doctrine and the doctrine of sovereign immunity, and it involves unique factual circumstances. Neither the Supreme Court nor the U.S. Court of Appeals for the D.C. Circuit has held that the fact that a person's data was taken is enough by itself to create standing to sue; a plaintiff who claims an actual injury must be able to connect it to the defendant's actions, and a

person who is pointing to a threat of future harm must show that the harm is certainly impending or that the risk is substantial. The fact that this is not just a data breach case, but that it is a data breach arising out of a particular sort of cyberattack against the United States, differentiates it from the majority of the legal precedent that arises in the context of retail establishments or other financial entities. Courts in those cases often make certain assumptions about the likelihood of future harm in order to find that the elements needed to initiate a case have been satisfied. Here, the usual assumptions about why the information was stolen and what is likely to be done with it in the future do not apply and cannot fill the gap. As for those plaintiffs who allege that they have already experienced an actual misuse of their credit card numbers or personal information, they cannot tie those disparate incidents to this breach. It may well be that the Supreme Court or the D.C. Circuit will someday announce that given the potential for harm inherent in any cyberattack, breach victims automatically have standing even if the harm has yet to materialize, and even if the purpose behind the breach and the nature of any future harm have yet to be discerned. But that has not happened yet, and the Court is not empowered to expand the limits of its own authority, so it cannot find that plaintiffs have standing based on this record.

Even if the Court were inclined to anticipate that this is where the law is heading, the problem runs deeper than standing. The right to bring a claim for damages under the Privacy Act is expressly limited to those who can demonstrate that they have suffered actual economic harm as a result of the government's statutory violation. The law is clear that the statute does not create a cause of action for those who have been merely aggrieved by, or are even actively worried about, the fact that their information has been taken. Neither the Administrative Procedure Act nor the Little Tucker Act supplies a cause of action against the government to enforce its information

security obligations, and no court has expressly recognized a right to data security arising under the Constitution.

Therefore, defendants' motions to dismiss will be granted, and both cases will be dismissed in their entirety. The Court finds, applying the case law it is required to follow, that neither set of plaintiffs has pled sufficient facts to demonstrate that they have standing. Moreover, even if they had the right to enter the courthouse, they did not bring a claim with them that the Court can hear. Plaintiffs have failed to overcome the arguments that the federal defendants are immune from suit under the Privacy Act and the Administrative Procedure Act, and that KeyPoint is shielded by government contractor immunity, so the Court lacks subject matter jurisdiction to hear those claims. Moreover, the Court finds that plaintiffs have failed to state claims upon which relief can be granted. Plaintiffs seek damages for improper disclosure of information and for a failure to maintain adequate safeguards under the Privacy Act, but they have not alleged that private information was "disclosed," as opposed to stolen, and they have not alleged facts to show that their claimed injuries were the result of the agency's failures. Plaintiffs have not stated a claim for breach of contract under the Little Tucker Act since they have not shown that OPM entered into a contract with them or that any contract was breached, and they have not alleged any violation of the United States Constitution.

TABLE OF CONTENTS

FACTUAL BACKGROUND

Defendant OPM is a federal agency that handles portions of the federal employee recruitment process. CAC ¶ 52; NTEU Compl. ¶¶ 10–11.[1] Defendant KeyPoint Government Solutions is a private contractor that conducts background investigations and security clearance checks on behalf of OPM. CAC ¶ 53.

I. The Data Breaches

The CAC plaintiffs allege that four breaches occurred in 2013 and 2014.

1 The NTEU complaint named OPM's Acting Director as the defendant in that case but sued her solely in her official capacity. NTEU Compl. ¶ 9. The Court will refer to the federal defendants named in the two complaints collectively as "OPM."

- On November 1, 2013, hackers "infiltrated" OPM's systems and stole "security system documents and electronic manuals" about the agency's systems, although no individual personal information was stolen. CAC ¶ 125; *see also* CAC ¶ 3.

- About a month later, in about December 2013, KeyPoint experienced a breach. "[A]n unknown person or persons obtained the user log-in credentials of a KeyPoint employee," and the credentials were used to "steal the personnel records of tens of thousands of Department of Homeland Security employees" from KeyPoint's systems. CAC ¶ 4.

- On May 7, 2014, hackers used "stolen KeyPoint credentials" to access OPM's network and install malware, creating "a conduit through which data could be exfiltrated." CAC ¶ 127. This breach "resulted in the theft of nearly 21.5 million background investigation records," which included "questionnaire forms containing highly sensitive personal, family, financial, medical, and associational information of Class members." CAC ¶ 129; *see also* NTEU Compl. ¶ 19.

- Finally, "[n]o later than October 2014," hackers attacked "OPM systems maintained in an Interior Department shared-services data center." CAC ¶ 131; *see also* NTEU Compl. ¶ 14. Hackers "use[d] the stolen KeyPoint credentials to access systems within OPM's network at will" and maintained access to OPM's network for "several months," removing "millions of personnel records," resulting in "the loss of approximately 4.2 million federal employees' personnel files." CAC ¶¶ 131, 133.

II. The Targeted Systems and Compromised Information

The CAC plaintiffs allege that the nature and scope of the data breaches "indicate that the intrusion was sophisticated, malicious, and carried out to obtain sensitive data for improper use." CAC ¶¶ 117, 128, 132. Both complaints allege that the cyberattacks removed data from OPM computer systems and databases, including OPM's Electronic Official Personnel Folder system and the Central Verification System. *See* CAC ¶¶ 64–65, 74, 130; NTEU Compl. ¶¶ 10–12 (describing relevant OPM systems).

The Electronic Official Personnel Folder system stores personnel files of federal employees. CAC ¶¶ 74, 130. These files include "birth certificates, job performance reports, resumes, school transcripts, military service records, employment history and benefits, and job applications that contain Social Security numbers and birthdates." CAC ¶ 74; NTEU Compl. ¶ 10.

The Central Verification System "contains most background and security clearance check information," including information from the three forms – Standard Form ("SF") 85, SF 85P, and SF 86 – that applicants for federal positions and security clearances must complete.[2] CAC ¶¶ 66, 69, 70. This system also contains information on security clearances, investigations, suitability determinations, background checks for those seeking access to federal facilities, and polygraph data. CAC ¶¶ 72, 73; NTEU Compl. ¶ 12.

III. OPM's Knowledge of the Deficiencies and Response to the Breaches

Both plaintiff groups allege that OPM "knew for several years" before the breaches that its "information security governance and management protocols contained material weaknesses that posed a significant threat to its systems." CAC ¶ 90; NTEU Compl. at 3 (alleging OPM had been "on notice of serious flaws in its data system security"). The Consolidated Amended Complaint states that the OPM Inspector General's annual audits of cybersecurity from 2007 to the present "found that OPM's information security policies and practices suffered from material weaknesses" that "pose an immediate risk to the security of assets or operations." CAC ¶¶ 81, 84, 86–88; NTEU Compl. at 3 (alleging the Inspector General's office had "identified numerous significant deficiencies, including deficiencies related to OPM's decentralized security governance structure, its failure to ensure that its information technology systems met applicable security standards, and

2 The federal government uses SF 85 for applicants seeking non-sensitive federal government or contractor positions and SF 85P for applicants seeking "public trust" federal government or contractor positions. CAC ¶¶ 69–70. It requires individuals who will need security clearances to complete the SF 86. CAC ¶ 66. SF 86 is a 127-page form and, according to the CAC, it seeks information about "applicants' psychological and emotional health history, police records, illicit drug and alcohol use history, Social Security numbers, birthdates, financial histories and investment records, children's and relatives' names, foreign trips taken and contacts with foreign nationals, past residences, names of neighbors and close friends (such as college roommates and co-workers), and the Social Security numbers and birthdates of spouses, children, and other cohabitants." CAC ¶ 67; *see also* NTEU Compl. ¶ 29.

its failure to ensure that adequate technical security controls were in place for all servers and databases").

After learning of the breaches, OPM issued a series of announcements to the public and affected individuals. With each revelation, the reported scope of the breach and the number of people affected increased.

On April 27, 2015, OPM notified "more than 48,000 federal employees that their personal information might have been exposed in the KeyPoint Breach." CAC ¶ 120. On June 4, 2015, it announced that it had experienced a data breach that "resulted in the exposure and theft of the [government investigation information] of approximately 4.2 million current, former, and prospective federal employees and contractors." CAC ¶ 138. On June 12, 2015, OPM acknowledged that the scope of breach was broader than previously disclosed and that "as many as 14 million current, former, and prospective federal employees and contractors" were affected. CAC ¶ 139. On July 9, 2015, OPM announced that the information "of approximately 21.5 million people had been exposed and stolen in the May 2014 breach," including the theft of 1.1 million fingerprints. CAC ¶ 140. Of the 21.5 million people affected, 19.7 million had undergone background checks. The other 1.8 million records concerned "mostly job applicants' spouses, children, and other cohabitants." CAC ¶ 140. On September 23, 2015, OPM announced that not 1.1 million, but approximately 5.6 million, fingerprints had been stolen. CAC ¶ 141.

The agency notified each individual whose private information had been compromised and offered free identity theft protection services at "a combined cost of approximately $154 million . . . for either 18 months or three years, depending on the amount and sensitivity of the compromised [information]." CAC ¶¶ 148, 150.

IV. Plaintiffs' Alleged Harm

The CAC plaintiffs allege that each of the thirty-eight named plaintiffs submitted sensitive personal information to the federal government that was compromised in the breaches. *See* CAC ¶¶ 10, 13–50; *see also* CAC ¶ 1. The NTEU plaintiffs allege that the three named plaintiffs and an unknown number of NTEU members were "identified by OPM as having been affected by the breaches." NTEU Compl. ¶ 59. Plaintiffs assert that the data breaches occurred as a result of defendants' failure to secure their systems, CAC ¶ 1, and that all of the putative class members are subject to a continuing risk of additional exposure since that failure is ongoing. CAC ¶ 7. The complaints allege that plaintiffs have sustained and will continue to sustain "economic loss and other harm," CAC ¶ 163; that they have suffered "stress," CAC ¶¶ 13, 18, 19, 22–25, 28, 30–31, 35, 37, 42–44, 46, 50; or a loss to their "sense of security," NTEU Compl. ¶ 78; and that they face an increased risk of expending time and money dealing with such consequences as identity theft and fraud in the future. CAC ¶ 163.

The complaints contain a range of allegations concerning the nature of the particular harm suffered by class members.

A. Actual Identity Theft or Credit Card Fraud

A number of plaintiffs allege that they have experienced actual identity theft or credit card fraud.

- Fourteen CAC plaintiffs and one of the three NTEU plaintiffs allege that at some point after they were informed of the breaches, they learned that unauthorized charges had been made to their existing credit card accounts or that fraudulent accounts were opened in their names. *See* CAC ¶¶ 13, 16, 19, 22, 28–31, 38, 39, 41, 45, 49, 50; NTEU Compl. ¶ 84.

- Four CAC plaintiffs allege that they experienced unauthorized credit inquiries. CAC ¶¶ 13, 14, 29, 31.

- Six CAC plaintiffs and one NTEU plaintiff allege that fraudulent tax returns were filed in their names. CAC ¶¶ 14, 21, 24, 28, 31, 32; NTEU Compl. ¶ 79.

- Four CAC plaintiffs allege that there was some other improper use of their own or a family member's Social Security number. CAC ¶¶ 14, 17, 41, 50.

B. Risk of Future Identity Theft and Other Harm Associated with that Risk

Both sets of plaintiffs claim that they have suffered harm as result of the breaches because they face an increased risk of identity theft in the future. CAC ¶¶ 7, 210; NTEU Compl. ¶ 92. Nearly all of the named CAC plaintiffs – thirty-four out of thirty-eight – allege that after learning about the breaches, they devoted some time and effort to preventing future identity theft. *See, e.g.*, CAC ¶¶ 13–22, 25–34, 36–44, 46–50 (alleging that exposure to the breach caused plaintiffs to review their financial accounts or credit reports with greater frequency, or that they placed freezes on their credit). Of those plaintiffs, seven allege that they spent money to purchased credit monitoring and protection services or incurred other expenses to prevent future identity theft. *See, e.g.*, CAC ¶¶ 17, 21, 25, 34, 41. And numerous plaintiffs allege that they "suffer stress" due to their concerns about future identity theft or a sense of vulnerability to some other harm. *See* CAC ¶¶ 18–19, 22–25, 28, 35, 37, 43–44 (expressing concerns for their safety or the safety of their family members); CAC ¶¶ 18–30, 43, 46 (expressing concern about an inability to obtain a security clearance in the future); CAC ¶¶ 19, 23–24, 42–44 (expressing fear about future identity theft); CAC ¶¶ 19, 31, 50 (alleging "stress resulting from concerns that her exposure to the Data Breaches will adversely affect her minor children's future"); *see also* NTEU Compl. ¶ 94 (expressing anxiety over the effect the data breaches will have on them, their families, friends, and other associates).

PROCEDURAL HISTORY

A number of lawsuits were filed around the country after the data breaches at OPM and KeyPoint were announced. The United States Judicial Panel on Multidistrict Litigation transferred all actions that were pending elsewhere to this Court for coordinated or consolidated proceedings

pursuant to 28 U.S.C. § 1407 [Dkt. # 1], and plaintiffs filed two amended complaints, which are the operative documents in this matter. *See* Order (Dec. 15, 2015) [Dkt. # 19].

The plaintiffs in the Consolidated Amended Complaint[3] assert that OPM violated the Privacy Act, the Little Tucker Act, and the Administrative Procedure Act ("APA"), and that KeyPoint is liable for negligence, negligent misrepresentation and concealment, invasion of privacy, breach of contract, and violations of the Fair Credit Reporting Act and various state statutes governing unfair and deceptive trade practices and data security. CAC ¶¶ 175–275. They seek declaratory and injunctive relief against both defendants. CAC at 75–76 (Prayer for Relief).

OPM and KeyPoint each filed motions to dismiss the CAC, arguing that the Court lacks subject matter jurisdiction under Federal Rule of Civil Procedure 12(b)(1) because plaintiffs do not have standing and defendants are shielded by sovereign immunity, and that plaintiffs failed to state a claim under Rule 12(b)(6). *See* KeyPoint's Mot. to Dismiss CAC & Mem. of Law in Supp. [Dkt. # 70] ("KeyPoint Mem."), Fed. Def.'s Mot. to Dismiss CAC and Mem. of P. & A. in Supp. [Dkt. # 72] ("OPM's Mem."); Pls.' Consol. Opp. to Defs.' Mots. To Dismiss [Dkt. # 82] ("CAC Pls.' Opp."); KeyPoint's Reply [Dkt. # 86]; Fed. Def.'s Reply [Dkt. # 87].

The NTEU plaintiffs assert a single claim against the Acting Director of OPM, alleging that the agency violated their constitutional right to informational privacy. NTEU Compl. ¶¶ 95–98. They seek declaratory and injunctive relief. NTEU Compl. at 34–35 (Request for Relief).

---

3 The CAC defines the class to include current, former, and prospective federal government employees and contractors, their family members and cohabitants, whose information was compromised as a result of the data breaches, and excludes defendants' senior officers, officials, and executives and their immediate family members, and "judicial officers to whom this case is assigned and their respective staffs." CAC ¶ 165.

OPM has moved to dismiss the NTEU complaint for lack of standing and for failure to state a claim.[4] *See* Fed. Defs.' Mot. to Dismiss NTEU Compl. [Dkt. # 81]; Mem. in Supp. [Dkt. # 81-1]; NTEU Pls.' Opp. to OPM's NTEU Mot. [Dkt. # 84] ("NTEU's Opp."); Fed. Def.'s Reply Mem. in Supp. of Mot. to Dismiss [Dkt. # 91].[5]

The Court heard oral argument on the motions, and the motions are fully briefed.

STANDARD OF REVIEW

In evaluating a motion to dismiss under either Rule 12(b)(1) or 12(b)(6), the Court must "treat the complaint's factual allegations as true . . . and must grant plaintiff 'the benefit of all inferences that can be derived from the facts alleged.'" *Sparrow v. United Air Lines, Inc.*, 216 F.3d 1111, 1113 (D.C. Cir. 2000) (internal citations omitted), quoting *Schuler v. United States*, 617 F.2d 605, 608 (D.C. Cir. 1979); *see also Am. Nat'l Ins. Co. v. FDIC*, 642 F.3d 1137, 1139 (D.C. Cir. 2011). Nevertheless, the Court need not accept inferences drawn by the plaintiff if those inferences are unsupported by facts alleged in the complaint, nor must the Court accept plaintiff's legal conclusions. *Browning v. Clinton*, 292 F.3d 235, 242 (D.C. Cir. 2002).

I. Lack of Subject Matter Jurisdiction

Under Rule 12(b)(1), the plaintiff bears the burden of establishing jurisdiction by a preponderance of the evidence. *See Lujan v. Defs. of Wildlife*, 504 U.S. 555, 561 (1992); *Shekoyan*

---

4 OPM also asserts that plaintiffs have failed to identify any statute that would waive sovereign immunity and enable the Court to order the agency to pay for lifetime credit monitoring. OPM's Mem. at 27–28.

5 *See also* Joint Omnibus Notice of Supp. Auth. [Dkt. # 95]; Notice of Recent Decision [Dkt. # 99]; Def. KeyPoint's Notice of Suppl. Citations [Dkt. # 102]; Pls.' Resp. to Def. KeyPoint's Notice of Suppl. Citations [Dkt. # 103]; Notice of Suppl. Auth. [Dkt. # 106], Resp. to Notice of Suppl. Auth. [Dkt. # 107], Resp. to Notice of Suppl. Auth. [Dkt. # 108], Notice of Recent Decision [Dkt. # 109], Resp. to Notice of Recent Decision [Dkt. # 110], Notice of Supp. Auth. [Dkt. # 111], NTEU Pls.' Supp. Submission [Dkt. # 112], Fed. Def. OPM's Suppl. Submission regarding *Attias v. CareFirst, Inc.* [Dkt. # 113], Def. KeyPoint's Suppl. Submission regarding *Attias v. CareFirst, Inc.* [Dkt. # 114], and Class Pls.' Suppl. Submission [Dkt. # 115].

v. Sibley Int'l Corp., 217 F. Supp. 2d 59, 63 (D.D.C. 2002). Federal courts are courts of limited jurisdiction and the law presumes that "a cause lies outside this limited jurisdiction." *Kokkonen v. Guardian Life Ins. Co. of Am.*, 511 U.S. 375, 377 (1994); *see also Gen. Motors Corp. v. EPA*, 363 F.3d 442, 448 (D.C. Cir. 2004) ("As a court of limited jurisdiction, we begin, and end, with an examination of our jurisdiction."). "[B]ecause subject-matter jurisdiction is 'an Art[icle] III as well as a statutory requirement . . . no action of the parties can confer subject-matter jurisdiction upon a federal court.'" *Akinseye v. District of Columbia*, 339 F.3d 970, 971 (D.C. Cir. 2003), quoting *Ins. Corp. of Ir., Ltd. v. Compagnie des Bauxites de Guinee*, 456 U.S. 694, 702 (1982).

When considering a motion to dismiss for lack of jurisdiction, unlike when deciding a motion to dismiss under Rule 12(b)(6), the court "is not limited to the allegations of the complaint." *Hohri v. United States*, 782 F.2d 227, 241 (D.C. Cir. 1986), *vacated on other grounds*, 482 U.S. 64 (1987). Rather, "a court may consider such materials outside the pleadings as it deems appropriate to resolve the question [of] whether it has jurisdiction to hear the case." *Scolaro v. D.C. Bd. of Elections & Ethics*, 104 F. Supp. 2d 18, 22 (D.D.C. 2000), citing *Herbert v. Nat'l Acad. of Scis.*, 974 F.2d 192, 197 (D.C. Cir. 1992); *see also Jerome Stevens Pharm., Inc. v. FDA*, 402 F.3d 1249, 1253 (D.C. Cir. 2005).

Furthermore, when a government agency is the defendant, additional jurisdictional considerations apply. The United States is not amenable to suit in the federal courts absent an express waiver of sovereign immunity. *Anderson v. Carter*, 802 F.3d 4, 8 (D.C. Cir. 2015), citing *United States v. Mitchell*, 463 U.S. 206, 212 (1983). Sovereign immunity is "jurisdictional in nature." *Perry Capital LLC v. Mnuchin*, 864 F.3d 591, 619 (D.C. Cir. 2017), quoting *FDIC v. Meyer*, 510 U.S. 471, 475 (1994). When it has not been waived, sovereign immunity shields the federal government, its agencies, and federal officials acting in their official capacities from suit.

Meyer, 510 U.S. at 475 (the federal government and its agencies); *Kentucky v. Graham*, 473 U.S. 159, 166–67 (1985) (federal officials in their official capacities).

II. Failure to State a Claim

"To survive a [Rule 12(b)(6)] motion to dismiss, a complaint must contain sufficient factual matter, accepted as true, to 'state a claim to relief that is plausible on its face.'" *Ashcroft v. Iqbal*, 556 U.S. 662, 678 (2009), quoting *Bell Atl. Corp. v. Twombly*, 550 U.S. 544, 570 (2007). In *Iqbal*, the Supreme Court reiterated the two principles underlying its decision in *Twombly*: "First, the tenet that a court must accept as true all of the allegations contained in a complaint is inapplicable to legal conclusions," and "[s]econd, only a complaint that states a plausible claim for relief survives a motion to dismiss." *Id.* at 678–79.

A claim is facially plausible when the pleaded factual content "allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged." *Id.* at 678, citing *Twombly*, 550 U.S. at 556. "The plausibility standard is not akin to a 'probability requirement,' but it asks for more than a sheer possibility that a defendant has acted unlawfully." *Id.*, quoting *Twombly*, 550 U.S. at 556. A pleading must offer more than "labels and conclusions" or a "formulaic recitation of the elements of a cause of action," *id.*, quoting *Twombly*, 550 U.S. at 555, and "[t]hreadbare recitals of the elements of a cause of action, supported by mere conclusory statements, do not suffice." *Id.*, citing *Twombly*, 550 U.S. at 555.

When considering a motion to dismiss under Rule 12(b)(6), the Court is bound to construe a complaint liberally in the plaintiff's favor, and it should grant the plaintiff "the benefit of all inferences that can be derived from the facts alleged." *Kowal v. MCI Commc'ns Corp.*, 16 F.3d 1271, 1276 (D.C. Cir. 1994). Nevertheless, the Court need not accept inferences drawn by the plaintiff if those inferences are unsupported by facts alleged in the complaint, nor must the Court accept plaintiff's legal conclusions. *See id.*; *see also Browning*, 292 F.3d at 242. In ruling upon a

motion to dismiss for failure to state a claim, a court may ordinarily consider only "the facts alleged in the complaint, documents attached as exhibits or incorporated by reference in the complaint, and matters about which the Court may take judicial notice." *Gustave-Schmidt v. Chao*, 226 F. Supp. 2d 191, 196 (D.D.C. 2002), citing *EEOC v. St. Francis Xavier Parochial Sch.*, 117 F.3d 621, 624–25 (D.C. Cir. 1997).

ANALYSIS

Defendants seek to dismiss both complaints for lack of subject matter jurisdiction on the grounds that plaintiffs lack standing and that there has not been a valid waiver of sovereign immunity, and they have also moved to dismiss for failure to state a claim. Courts must determine whether they have jurisdiction to hear a case before considering whether plaintiffs have failed to state a claim. *Hancock v. Urban Outfitters*, 830 F.3d 511, 513 (D.C. Cir. 2016) ("Federal courts cannot address the merits of a case until jurisdiction – the power to decide – is established.") Accordingly, the Court will address the issue of plaintiffs' standing first.

I. Plaintiffs Do Not Have Standing.

"To state a case or controversy under Article III, a plaintiff must establish standing." *Ariz. Christian Sch. Tuition Org. v. Winn*, 563 U.S. 125, 133, citing *Allen v. Wright*, 486 U.S. 737, 751 (1984); *see also Lujan*, 504 U.S. at 560. Standing is a necessary predicate to any exercise of federal jurisdiction; if it is lacking, then the dispute is not a proper case or controversy under Article III, and federal courts have no subject matter jurisdiction to decide the case. *Dominguez v. UAL Corp.*, 666 F.3d 1359, 1361 (D.C. Cir. 2012). Plaintiffs must demonstrate standing for each claim they assert. *Daimler Chrysler Corp. v. Cuno*, 547 U.S. 332, 352 (2006) (holding that "our standing cases confirm that a plaintiff must demonstrate standing for each claim he seeks to press"); *see also Friends of the Earth, Inc. v. Laidlaw Envtl. Servs.*, 528 U.S. 167, 185 (2000). And each plaintiff must demonstrate standing, including in a putative class action. *See Lujan*, 504 U.S. at

563 ("The 'injury in fact' test . . . requires that the party seeking review be himself among the injured."), quoting *Sierra Club v. Morton*, 405 U.S. 727, 734 (1972); *see also Warth v. Seldin*, 422 U.S. 490, 502 (1975) (named plaintiffs in a putative class action "must allege and show that they personally have been injured, not that injury has been suffered by other, unidentified members of the class to which they belong and which they purport to represent").

The party invoking federal jurisdiction bears the burden of establishing standing. *Lujan*, 504 U.S. at 561. When reviewing the standing question, the Court must be "careful not to decide the questions on the merits for or against the plaintiff, and must therefore assume that on the merits the plaintiffs would be successful in their claims." *In re Navy Chaplaincy*, 534 F.3d 756, 760 (D.C. Cir. 2008), quoting *City of Waukesha v. EPA*, 320 F.3d 228, 235 (D.C. Cir. 2003).

A. Legal Framework

To establish constitutional standing, plaintiffs must show that (1) they have suffered an "injury in fact," (2) the injury is "fairly . . . trace[able] to the challenged action of the defendant," and (3) it is "'likely,' as opposed to merely 'speculative,' that the injury will be 'redressed by a favorable decision.'" *Lujan*, 504 U.S. at 560–61 (citations omitted); *see also Friends of the Earth, Inc.*, 528 U.S. at 180–81.

1. Individual Standing

Individual plaintiffs must satisfy all three of the *Lujan* elements. To allege the first element, injury in fact, plaintiffs must demonstrate that they "suffered 'an invasion of a legally protected interest' that is 'concrete and particularized' and 'actual or imminent, not conjectural or hypothetical.'" *Spokeo, Inc. v. Robins*, 136 S. Ct. 1540, 1548 (2016), quoting *Lujan*, 504 U.S. at 560.

To be "concrete," the injury "must actually exist," meaning that it is real, and not abstract, although concreteness is "not . . . necessarily synonymous with 'tangible.'" *Id.* at 1548–49. And

to be "particularized," the injury must affect a plaintiff "in a personal and individual way." *Id.* at 1548, quoting *Lujan*, 504 U.S. at 560 n.1.

Further, the injury must be "actual," or it must be "imminent" – that is, the "threatened injury must be certainly impending to constitute injury in fact." *Clapper v. Amnesty Int'l USA*, 568 U.S. 398, 410 (2013); *see also Pub. Citizen, Inc. v. Nat'l Highway Traffic Safety Admin.*, 489 F.3d 1279, 1293 (D.C. Cir. 2007) (the injury must be "certainly impending and immediate – not remote, speculative, conjectural, or hypothetical"). Or, as the D.C. Circuit has recently pointed out, the Supreme Court has "also noted that in some cases it has 'found standing based on a substantial risk that the harm will occur.'" *Attias v. CareFirst, Inc.*, 865 F.3d 620, 626 (D.C. Cir. 2017), quoting *Clapper*, 568 U.S. at 414 n.5.

To establish the second element, and show that an injury is "fairly traceable" to a defendant's action, a plaintiff must allege a causal connection between the alleged injury and the defendant's conduct at issue. *Ctr. for Law & Educ. v. Dep't of Educ.*, 396 F.3d 1152, 1157 (D.C. Cir. 2005). The alleged harm cannot be "the result of the independent action of some third party not before the court." *Food & Water Watch v. EPA*, 5 F. Supp. 3d 62, 73 (D.D.C. 2013), quoting *Lujan*, 504 U.S. at 560–61. "But Article III standing does not require that the defendant be the most immediate cause, or even a proximate cause, of the plaintiffs' injuries; it requires only that those injuries be 'fairly traceable' to the defendant." *Attias*, 865 F.3d at 629.

Finally, to be "redressable," the alleged injury must be one that a court order in favor of the plaintiff would be "likely" to address the harm. *Lujan*, 504 U.S. at 560–61.

2. Organizational Standing

The standing requirements that apply to individuals also apply to organizations, such as the two unions that are plaintiffs: AFGE and NTEU. *Nat'l Treasury Emps. Union v. United States*, 101 F.3d 1423, 1427 (D.C. Cir. 1996), citing *Havens Realty Corp. v. Coleman*, 455 U.S. 363, 378

(1982). Organizations may assert standing on their own behalf under certain circumstances, or they may seek representational standing on behalf of their members. *Nat'l Ass'n of Home Builders v. EPA*, 667 F.3d 6, 12 (D.C. Cir. 2011).

To assert organizational standing, an organization must allege "such a 'personal stake' in the outcome of the controversy as to warrant the invocation of federal-court jurisdiction," and must show "concrete and demonstrable injury to the organization's activities – with [a] consequent drain on the organization's resources – constitut[ing] . . . more than simply a setback to the organization's abstract social interests." *Nat'l Taxpayers Union, Inc. v. United States*, 68 F.3d 1428, 1433 (D.C. Cir. 1995) (alterations in original), quoting *Havens Realty*, 455 U.S. at 378–79.

To assert representational standing on behalf of its members, an organization must show that "(a) its members would otherwise have standing to sue in their own right; (b) the interests it seeks to protect are germane to the organization's purpose; and (c) neither the claim asserted nor the relief requested requires the participation of individual members in the lawsuit." *Nat'l Ass'n of Home Builders*, 667 F.3d at 12, quoting *Ass'n of Flight Attendants-CWA v. U.S. Dep't of Transp.*, 564 F.3d 462, 464 (D.C. Cir. 2009).

B. Plaintiffs have Failed to Show that They have Article III Standing

Plaintiffs allege that some of them have incurred actual out-of-pocket expenses, that others have expended time and effort, and that others have experienced emotional distress or may be subject to identity theft or some other harm in the future. Plaintiffs also contend that all of them have suffered the injury of the breach itself. The Court is not persuaded that the factual allegations in the complaints are sufficient to establish constitutional standing.

1. Injury in Fact

a. Theft of Private Information Without More

At oral argument, counsel for the CAC plaintiffs took to the lectern to advocate a new basis for standing that had not been set forth in any prior consolidated pleading: that the release or theft of private information – as opposed to any actual or even threatened misuse of that information – is itself the injury in fact for standing purposes in a Privacy Act case. Hr'g Tr. [Dkt. # 98] at 26–28 ("I don't think you get to the question of imminence because we're not talking about a risk of future injury; the injury happened; . . . . [W]e're not premising the Court's Article III standing on a risk of future injury, we're premising it on an injury that has occurred and has been recognized at common law."). In other words, if your personal information was included in the material accessed in a data breach, you automatically have standing to bring an action predicated on a violation of the Privacy Act. *See* NTEU Compl. ¶ 76 (alleging that harm "occurred the moment that [plaintiffs'] inherently personal information . . . was taken by unauthorized intruders from OPM's databases").

While one could make a compelling argument that this would be an appropriate principle to adopt in data breach cases given the volume, sensitivity, and vulnerability of computerized private information, the Court is not writing a law review article. Therefore, it cannot ignore the fact that neither the Supreme Court nor the D.C. Circuit has embraced this categorical approach to standing to date. In the absence of authority to support plaintiffs' proposal, it is not up to the Court to expand the constitutional limitations on its jurisdiction on its own initiative, particularly when considerations of sovereign immunity and separation of powers concerns are also involved. *See Spokeo*, 136 S. Ct. at 1547 (the standing doctrine developed "to ensure that federal courts do not exceed their authority as it has been traditionally understood"). Therefore, the Court believes that it is constrained to find that plaintiffs cannot predicate standing on the basis of the breach alone.

At the hearing, plaintiffs pointed to *Doe v. Chao*, 540 U.S. 614 (2004), as support for the notion that "the release itself is the injury." Hr'g Tr. at 32. But the case does not stand for that proposition. In *Doe*, the Supreme Court held that a plaintiff must suffer actual damages to bring a claim under Privacy Act. *Id.* at 616. In the course of the opinion, the Court noted that the petitioner had argued against that interpretation; he pointed out that in subsection (g)(1) of the statute, Congress expressly granted any individual who suffered an "adverse effect" as a result of an agency's failure to comply with the Act the right to sue that agency without any further limitation. *Id.* at 624. In responding to that argument, the Court stated:

> [T]he reference in § 552a(g)(1)(D) to 'adverse effect' acts as a term of art identifying a potential plaintiff who satisfies the injury-in-fact and causation requirements of Article III standing, and who may consequently bring a civil action without suffering dismissal for want of standing to sue. That is, an individual subjected to an adverse effect has injury enough to open the courthouse door, but without more has no cause of action for damages under the Privacy Act.

Id. at 624–25.

That discussion does not necessarily mean that anyone whose information was included in a data breach automatically "has injury enough to open the courthouse door;" the statutory reference to an adverse "effect" seems to imply that there is a need for individualized consequences beyond the mere fact that a release took place, and Doe himself alleged that he suffered from

emotional distress.[6] *See id*. at 617–18. And the Court in *Doe* did not purport to answer the question of whether the release of private information alone is an "adverse effect."

Plaintiffs also insisted that this issue was "specifically considered" in *In re Department of Veterans Affairs Data Theft Litigation*, No. 06-0506, 2007 WL 7621261 (D.D.C. Nov. 16, 2007) ("*VA Data Theft Litig.*"). Hr'g Tr. at 27 ("[T]he Court said yes, that's an adverse effect, that gives rise to Article III standing."); *see also* Hr'g Tr. at 27–28 ("[T]he injury occurs at that moment. And this is a precise issue that the Court looked at in the *VA Laptops* case."). It is true that the *VA Data Theft* opinion denied a motion to dismiss for lack of subject matter jurisdiction. But the court in that case did not consider at any point whether a release of data in and of itself constitutes an injury that would give rise to standing.

The VA plaintiffs did not rely on the fact of the breach as the foundation for their suit; they specifically alleged that they had suffered pecuniary and emotional harm as a result of the theft, including the cost of credit reports and credit monitoring services, and mental anguish. *VA Data Theft Litig.*, 2007 WL 7621261, at *3. The government moved to dismiss on the grounds that these allegations of harm were not tied to any particular plaintiff and that they were insufficiently

6 At another point in the hearing, one of the other attorneys for the plaintiffs pointed the Court to the dissent in *Doe*, in which Justice Ginsburg argued against the ruling by the majority that one must suffer economic loss in addition to emotional distress to advance a Privacy Act claim. Hr'g Tr. at 37. In her opinion, the Justice emphasized that "Doe has standing to sue . . . based on 'allegations that he was "torn . . . all to pieces" and "greatly concerned and worried" because of the disclosure of his Social Security number and its potentially "devastating" consequences,'" and she reasoned that the statute should call for no more for the claim to move forward. 540 U.S. at 641 (Ginsburg, J., dissenting) (quoting *Doe*, 540 U.S. at 617–18). The Justice's observation that the distraught Mr. Doe had standing does not bear on the question of whether these plaintiffs have standing by virtue of the release of their data even if they suffered no further consequences at all.

detailed. *Id.* The court simply found the general allegations of monetary harm to be sufficient,[7] and it did not predicate its decision on the mere fact that the data had gone missing. *Id.*

At the hearing, plaintiffs appeared to be drawing on the concepts underlying the Supreme Court's decision in *Spokeo* when they maintained that they had standing simply because they were the victims of a Privacy Act violation:

> As I understand the Privacy Act, it's really codifying common law privacy protection principles . . . . [T]his isn't like a procedural violation case because the harm has occurred upon the release, and the reason is that the underlying claim is rooted in the common law protection of privacy principles. And so it was recognized at common law that if your private information was made public or there was an intrusion on your right to seclusion, the injury occurs at that moment.

Hr'g Tr. at 26–28; *see Spokeo*, 136 S. Ct. at 1549. Plaintiffs acknowledged that *Spokeo* requires a would-be plaintiff to make a showing of harm, Hr'g Tr. at 28, but they maintained that the showing had been made in this case because it is inherent in the nature of the allegations.

> [I]t does cause harm . . . . [T]he harm is recognized at common law. So it's not like a situation – let's say it's a Truth in Lending Act claim and you have the right so some disclosure . . . [and] it never had any impact on you whatsoever. That's *Spokeo*. This is different. This is a common law right to the protection of your private facts. That right is infringed at the point when the release occurs. And the causation issue doesn't enter in . . . .

Hr'g Tr. at 28–29.

What plaintiffs are suggesting, then, is that the challenged action that makes the defendant liable – in this case, a failure to prevent a breach – is also the harm: the loss of the data is the whole story. But adopting that approach would collapse the standing analysis in data breach cases

---

7 That aspect of the *VA Data Theft* holding has limited precedential value given the subsequent Supreme Court rulings in *Clapper*, 568 U.S. 398, and *FAA v. Cooper*, 566 U.S. 284 (2012). It is true that in *Cooper*, the Supreme Court considered the requirements for a Privacy Act claim without addressing the standing question. While plaintiffs argue that means the Court was not troubled by the standing issue in that case, *see* Hr'g Tr. at 37, the opinion supplies no guiding principles to be applied here.

entirely, answering both of the injury-in-fact inquiries – is the harm actual or imminent and is it concrete and particularized? – and the causation and redressability inquiries – is the injury fairly traceable to the defendant's unlawful action and would the relief sought cure the harm? – with a single allegation: my data was involved. Adopting such a tautological approach would effectively eliminate the requirement to establish the elements of Article III standing in data breach cases brought against the government, and while the Supreme Court may be headed in that direction, it has not arrived there yet.

A close reading of the majority opinion in the *Spokeo* case reveals that the Court did not relax traditional standing requirements – if anything, *Spokeo* reaffirmed the constitutional underpinnings of the doctrine – and it stopped short of the theory plaintiffs advance here. The holding addresses only one prong of the standing analysis – concreteness – and it left critical aspects of even that issue open for further development. While the Court opined that a violation of a statute enacted to protect rights that have traditionally been recognized in our courts could give rise to a concrete injury without more in some circumstances, it cautioned that it would not do so in all circumstances. And disappointing commentators everywhere, it left the delineation of the boundary for another day. Since isolated phrases from the opinion can point in different directions when lifted out of context, it is necessary to review the opinion of the Court in some detail. But the message to be gleaned from that analysis is that the holding underscored that an injury in fact predicated on a statutory violation – even a violation of a statute intended to protect

a traditionally recognized personal right – must carry with it a risk of "real harm."[8] *Spokeo*, 136 S. Ct. at 1549.

Spokeo is a firm that conducts searches of computerized databases to supply visitors to its website with information about the people they identify. *Spokeo*, 136 S. Ct. at 1544. The plaintiff, Robins, became aware that personal information that had been disseminated about him – including his age, marital status, and employment – was incorrect, and he instituted a class action against the company for violating the Fair Credit Reporting Act. *Id.* at 1546. The district court dismissed the action on the grounds that Robins had failed to allege the necessary injury in fact, but the Ninth Circuit reversed, finding that the allegation that Robins's own statutory rights had been violated was sufficient. *Id.* The Supreme Court sent the case back, complaining that the Ninth Circuit had considered only the "particularized" portion of the requirement that an injury be "concrete and particularized," and it called for the missing half of the review. *Id.* at 1549.

The *Spokeo* analysis begins by reciting the holding in *Lujan* that "the 'irreducible constitutional minimum' of standing consists of three elements": injury in fact, traceability, and redressability, *id.* at 1547, quoting *Lujan*, 504 U.S. at 560, and that a plaintiff must allege facts demonstrating each. *Id.*, citing *Warth*, 422 U.S. at 518. The Court reiterated that "[i]njury in fact is a constitutional requirement, and 'it is settled that Congress cannot erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing.'" *Id*. at 1547–48, quoting *Raines v. Byrd*, 52 U.S. 811, 820 n.3 (1997). The Court listed

8 If the loss of data in and of itself is not an injury in fact, then for the same reasons, plaintiffs' allegation that they are subject to a risk of another breach in the future because the security flaws have yet to be rectified, *see* CAC ¶ 7, does not allege a threat of future harm that constitutes an injury in fact.

the multiple components of the injury-in-fact element, but it went on to discuss just the particularization and concreteness requirements. *Id.* at 1548–50.

The Court repeated that "for an injury to be 'particularized,' it must affect the plaintiff in a 'personal and individual way.'" *Id.* at 1548, quoting *Lujan*, 504 U.S. at 560 n.1. But it emphasized that particularization is "not sufficient. An injury in fact must also be 'concrete.'" *Id.* ("We have made it clear time and time again that in injury in fact must be both concrete and particularized."). The opinion went on to explain that while the injury must be "'*de facto*,' that is, it must actually exist," and that it must be "'real' and not 'abstract,'" it is not necessary that the injury be tangible to be concrete. *Id.* at 1548-49 ("[W]e have confirmed in many of our previous cases that intangible injuries can nevertheless be concrete.").

How would one go about identifying an intangible harm that constitutes a concrete injury in fact? Writing for the Court, Justice Alito explained that "both history and the judgment of Congress play important roles." *Id.* at 1549.

> [I]t is instructive to consider whether an alleged intangible harm has a close relationship to a harm that has traditionally been regarded as providing a basis for a lawsuit in English or American courts. In addition, because Congress is well-positioned to identify intangible harms that meet minimum Article III requirements, its judgment is also instructive and important.

Id. (citations omitted). At the same time, the opinion cautioned that "Congress' role in identifying and elevating intangible harms does not mean that a plaintiff *automatically* satisfies the injury-in-fact requirement whenever a statute grants a person a statutory right and purports to authorize that person to sue to vindicate that right." *Id.* (emphasis added).

> Article III standing requires a concrete injury even in the context of a statutory violation. For that reason, Robins could not, for example, allege a bare procedural violation, divorced from any concrete harm and satisfy the injury-in-fact requirement . . . .

Id. Turning back to the other hand, Justice Alito went on:

> This does not mean, however, that the risk of real harm cannot satisfy the requirement of concreteness. For example, the law has long permitted recovery by certain tort victims even if their harms may be difficult to prove or measure. Just as the common law permitted suit in such instances, the violation of a procedural right granted by statute can be sufficient *in some circumstances* to constitute injury in fact. In other words, a plaintiff *in such a case* need not allege any additional harm beyond the one Congress has identified.

Id. (emphasis added) (emphasis and citations omitted).

Applying all of those general principles to the case before him, Justice Alito derived two conclusions: that Congress clearly intended to prevent the harm that had befallen Robins, i.e., the dissemination of false information, when it enacted the provisions that were alleged to have been violated, but that Robins could not meet the requirements of Article III standing simply by alleging a "bare procedural violation." *Id.* Since it was possible that a violation of one of the statute's procedural requirements could result in *no* harm, the case was remanded to the Ninth Circuit to address "whether the particular procedural violations alleged . . . entail a degree of risk sufficient to meet the concreteness requirement." *Id.* at 1550.

According to plaintiffs, their allegation of a statutory violation supplies a basis for standing since they suffered the harm of an intangible violation of their privacy – a harm traditionally recognized at common law that Congress specifically intended to protect when it enacted the statute in question. Hr'g Tr. at 28–29. But that is exactly what the Supreme Court found to be insufficient in *Spokeo* without a further showing that real harm, albeit even intangible harm, would

necessarily follow.[9] And the opinion was specifically limited to a consideration of the "concrete and particularized" element of an injury in fact; the Supreme Court did not hold that once a plaintiff has alleged an injury to a traditionally recognized intangible right that satisfies the concreteness requirement, there is no longer any need to establish that the harm is actual or imminent, or to satisfy the traceability or redressability requirements.

This reading of *Spokeo* is consistent with the Circuit precedent that the Court is bound to follow; the Court of Appeals emphasized in *Hancock v. Urban Outfitters* that *Spokeo* did not alter the standing requirements. "*Spokeo* held that plaintiffs must have suffered an actual (or imminent) injury that is both particularized and 'concrete . . . even in the context of a statutory violation' . . . . For that reason, a plaintiff cannot 'allege a bare procedural violation, divorced from any concrete harm, and satisfy the injury-in-fact requirement of Article III.'" *Hancock*, 830 F.3d at 514, quoting *Spokeo*, 136 S. Ct. at 1549. In *Hancock*, there was no question that each of the plaintiffs was personally involved: each had been asked to provide her zip code during the course of a credit card transaction, and that information was entered into the retailer's sales register. *Id.*

9 Plaintiffs' counsel attempted to differentiate *Spokeo* – "it's not like a situation – let's say it's a Truth in Lending Act claim and you have some right to some disclosure and you never saw the disclosure . . . it never had any impact on you whatsoever. That's *Spokeo* . . . ." – but that characterization of the case was incorrect. Hr'g Tr. at 28–29. In *Spokeo*, Justice Alito specifically found that the complained of action *did* intrude on Robins's privacy rights, and he still resisted concluding that Robins automatically had standing, finding that the violation of a statutorily imposed procedure might not necessarily carry with it a risk of real harm that would satisfy the concreteness requirement. *Spokeo*, 136 S. Ct. at 1550. Plaintiffs allege two statutory violations here. They allege a "disclosure" in violation of the Privacy Act, CAC ¶¶ 175–85, but as set forth in section II.A.1.B. below, a theft does not qualify as a "disclosure." So the core of plaintiffs' claim is that OPM failed to comply with the requirements in the statute that it "establish appropriate . . . safeguards" to protect agency records. 5 U.S.C. § 552a(e)(10). The Court is hard pressed to assess the sufficiency of allegations in the complaint that such a failure necessarily entails a degree of risk sufficient to satisfy the concreteness requirement because this basis for standing is not set forth in the complaint, plaintiffs did not advance the theory in their papers, and they assumed at oral argument that no discussion of harm was required.

at 512. But the Court was clear that the allegation of a violation of the District of Columbia's Consumer Protection Act was not enough to create an injury in fact absent any allegation of a concrete consequence:

> The Supreme Court has been clear that the legislature "cannot erase Article III's standing requirements by statutorily granting the right to sue to a plaintiff who would not otherwise have standing" . . . . Instead, an asserted injury to even a statutorily conferred right "must actually exist," and must have "affect[ed] the plaintiff in a personal and individual way."

Id. at 514,[10] quoting *Spokeo*, 136 S. Ct. at 1547–48 (citations omitted); *see also Attias*, 865 F.3d at 626–27 (Court of Appeals relied on the sufficiency of allegations of future identity theft, and not the fact of the release of the data alone, as the basis for finding standing).

Plaintiffs seemed to find support in Justice Thomas's concurring opinion in *Spokeo*, Hr'g Tr. at 28, but Justice Thomas did not address the precise situation before the Court either. In agreeing with the decision to remand, he differentiated between a suit brought by an individual to vindicate a private right, and a suit seeking to vindicate a public right – a demand that a federal agency "follow the law." *Spokeo*, 136 S. Ct. at 1552 (Thomas, J., concurring). He said that in the second instance, there needs to be some personal impact on the plaintiff, and given separation of powers concerns, Congress cannot simply authorize private plaintiffs to enforce public rights without meeting all of the constitutionally based requirements. *Id.* But he differentiated that situation from a suit like the one in *Spokeo* in which a private plaintiff was seeking to enforce his own private rights against a private party: "[i]f Congress has created a private duty owed personally to Robins to protect *his* information, then the violation of the legal duty suffices for

10 The Court observed that neither *Hancock* plaintiff had alleged any invasion of privacy, increased risk of fraud or identity theft, or pecuniary or emotional injury, but it did not specifically address the question of whether an allegation of an invasion of privacy rights alone would suffice. 830 F.3d at 514.

Article III injury in fact." *Id.* at 1554 (Thomas, J., concurring).[11] Neither alternative quite mirrors the situation of a private plaintiff suing a federal defendant to vindicate a private right.

But more important, even if one assumes that the principles reviewed by the Justices would apply equally to cases against the government, the *Spokeo* discussion arose in the context of a statute that creates a private right of action for a statutory violation without the need for a showing of harm. *See id.* at 1553 (Thomas, J, concurring) ("Congress can create new private rights and authorize private plaintiffs to sue *based simply on the violation of those private rights*. A plaintiff seeking to vindicate a statutorily created private right need not allege actual harm beyond the invasion of that private right.") (emphasis added) (citation omitted); *see also id.* at 1549 ("[T]he violation of a procedural right granted by statute can be sufficient in some circumstances to constitute injury in fact . . . . [A] plaintiff in such a case need not allege any *additional* harm *beyond the one Congress has identified*.") (first emphasis in original, second emphasis added).

The Privacy Act is not that sort of statute. Congress carefully limited the remedies that would be available in a Privacy Act case, and it specifically added the requirement of a showing of actual harm beyond the statutory violation and its impact on one's privacy before the government would be required to answer in Court. So even if the Court were inclined to read the tea leaves and predict that the Supreme Court will eventually find that the bare allegation that a plaintiff was a victim of a data breach, without more, is enough to create standing to sue under the Privacy Act given the privacy rights involved, the victory for plaintiffs would be a hollow one. Because notwithstanding any invasion of privacy, before the Court may pierce the shield of sovereign immunity and exercise jurisdiction, it must consider still whether the complaint

11 The Court notes that the dissenters were of the firm belief that Robins had standing. *Spokeo*, 136 S. Ct. at 1554–56 (Ginsburg, J., dissenting).

plausibly alleges that the named plaintiffs suffered the actual damages necessary to require the government to submit to a Privacy Act claim, and as set forth further below, it does not.

And finally, even if the Court were to find that there is standing to sue under the Privacy Act because Congress authorized plaintiffs to sue to vindicate their private rights in that Act, that would only confer standing to bring the Privacy Act claim. Contrary to plaintiffs' suggestion, *see* Hr'g Tr. at 30,[12] it would not open the door for plaintiffs to advance the APA claims based on OPM's violation of the Federal Information Security Management Act ("FISMA"). *See Cuno*, 547 U.S. at 352; *Friends of the Earth*, 528 U.S. at 185. Congress did not establish a private right to sue under FISMA, and there is no basis to conclude that the statutory regime protecting all systems and records across the federal government was specifically intended to vindicate individual rights that are grounded in our history or tradition.

For all of these reasons, in the Court's view, standing in this case must rise or fall on the sufficiency of the allegations of actual or future harm set forth in the complaint, and it is necessary to undertake that analysis.[13]

b. Actual Identity Theft or Fraudulent Credit Card Activity

Twenty plaintiffs allege that they have already experienced identity theft or have been the victims of financial fraud. They describe unauthorized charges made to existing accounts or accounts fraudulently opened in their names, unauthorized inquiries made concerning their credit, fraudulent tax returns filed in their names, or other improper uses of their credit card or Social

12 "I thought standing was a gatekeeping doctrine that says, Do you have a right to be in court? . . . [T]o me, once you're in court, if you read cases, courts don't go through every claim . . . in the case and analyze standing separately for each one."

13 In any event, after the D.C. Circuit issued its opinion in *Attias*, and the Court called for supplemental briefing, plaintiffs reverted back to the theory articulated in their complaint: that all plaintiffs have standing based on the risk of future harm. Class Pls.' Supp. Submission [Dkt. # 115] at 4–5.

Security numbers. CAC ¶¶ 13, 14, 16, 17, 19, 21, 24, 26, 28–32, 38, 39, 41, 45, 49, 50; NTEU Compl. ¶¶ 80–84. For example:

- Plaintiff "King-Myers provided sensitive information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In May 2015, King-Myers learned that unauthorized charges of approximately $658 had been incurred on her debit card account. King-Myers has spent between 30 and 35 hours attempting to reverse these fraudulent transactions." CAC ¶ 38.

- Plaintiff Ryan Lozar provided sensitive information and received notice that his information was compromised. "Lozar thereafter learned that an unknown individual had opened a PayPal account in his name and received a $1000 cash advance. He also learned that an unidentified individual had opened a Best Buy account in his name and used it to purchase $3,500 worth of merchandise." Lozar spent many hours communicating with PayPal and Best Buy to dispute and resolve these fraudulent activities. CAC ¶ 39.

- Plaintiff Kimberly Winsor and her husband "provided sensitive personal information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. In April 2015, Winsor's husband learned from their bank that his debit card number had been used the make unauthorized purchases in Mississippi. On July 23, 2015, Winsor learned from their bank that her debit card had been used to make unauthorized purchases in Texas. On November 24, 2015, CSID informed Winsor that her 8 year old son's social security number had been used in California for an unknown purpose." CAC ¶ 50.[14]

Only two of these plaintiffs allege that they incurred out-of-pocket expenses related to actual identity theft. *See* CAC ¶ 22 (plaintiff "paid approximately $198 to a credit repair law firm for assistance in closing the fraudulent accounts and removing them from her credit report" and "expended approximately $50 to obtain copies of her credit report"); CAC ¶ 41 (plaintiff purchased credit repair services). None of the plaintiffs who allege that unauthorized charges were made to their accounts allege that they were held financially responsible for the charges, *see* CAC ¶¶ 13, 16, 19, 22, 28–31, 38–39, 41, 45, 49, 50; NTEU Compl. ¶ 80–84, and none who

14 The complaint does not specifically allege that the son's Social Security number was included in the "sensitive information" provided to the federal government in connection with Winsor's employment.

experienced other attempts to utilize their identity alleged that they incurred out-of-pocket costs other than fees paid to purchase credit monitoring, which will be addressed separately below.

A number of courts have held that to base standing on past actual harm, plaintiffs in a data breach case must allege not only that their personal data was misused, but also that they suffered economic loss as a result. *See, e.g.*, *Whalen v. Michael Stores Inc.*, 689 F. App'x 89, 90 (2d Cir. 2017) ("Whalen does not allege a particularized and concrete injury suffered from the attempted fraudulent purchases . . . ; she never was either asked to pay, nor did pay, any fraudulent charge."); *Burton v. MAPCO Exp., Inc.*, 47 F. Supp. 3d 1279, 1284–85 (N.D. Ala. 2014) (plaintiff alleged unauthorized charges on his debit card but had no standing because he did not allege that he had to pay the charges); *In re Barnes & Noble Pin Pad Litig.*, No. 12-cv-8617, 2013 WL 4759588, at *6 (N.D. Ill. Sept. 3, 2013) ("[Plaintiff] has not pled that actual injury resulted and that she suffered any monetary loss due to the fraudulent charge. . . . In order to have suffered an actual injury, she must have had an unreimbursed charge on her credit card."); *Hammond v. Bank of N.Y. Mellon Corp.*, No. 08-cv-6060, 2010 WL 2643307, at *8 (S.D.N.Y. June 25, 2010) (no Article III injury where plaintiff was not financially responsible for unauthorized credit card charge).

Other courts, including some in this district, have held that allegations that plaintiffs' data was misused state an injury in fact, even in the absence of any allegation that they suffered financial consequences as a result. *See In re Sci. Applications Int'l Corp. Backup Tape Data Theft Litig.*, 45 F. Supp. 3d 14, 25 (D.D.C. 2014) ("*SAIC*") (holding that the "handful" of the plaintiffs who claimed to have suffered actual identity theft "clearly suffered an injury" but ultimately holding they did not have standing because they failed to allege causation); *Welborn v. IRS*, 218 F. Supp. 3d 64, 76–77 (D.D.C. 2016) (holding that plaintiffs who alleged actual identity theft in the form

of false tax returns filed in their names pled injury in fact); *In re Zappos.com, Inc.*, MDL No. 2357, 2016 WL 2637810, at *3–*4 (D. Nev. May 6, 2016).

There is no controlling authority on whether plaintiffs alleging actual harm must allege economic losses from a data breach to show injury in fact. The D.C. Circuit's recent opinion in *Attias v. CareFirst* dealt with allegations of future harm only, and did not directly address the question. 865 F.3d at 626. The Court finds the *Michael Stores* line of cases to be persuasive, and it is inclined to agree that a plaintiff must allege unreimbursed out-of-pocket expenses from the alleged identity thefts to state an injury in fact. *See Michael Stores Inc.*, 689 F. App'x 89 (2d Cir. 2017); *Burton*, 47 F. Supp. 3d at 1280–81; *In re Barnes & Noble*, 2013 WL 4759588, at *3–*4; *Hammond*, 2010 WL 2643307, at *8. However, since the D.C. Circuit has recently stated that a substantial *threat* of identity theft can satisfy the "actual or imminent" prong of the injury-in-fact element, and that identity theft would constitute a concrete and particularized injury, *Attias*, 865 F.3d at 627–29, and it did not mention any need for an out-of-pocket loss, it appears that the Court of Appeals may well ultimately agree with those district judges who have ruled that identity theft is an actual injury, notwithstanding a lack of economic harm. So while this Court finds that only two of the plaintiffs have alleged any injury in fact, it will also go on, as the *SAIC* court did, to consider whether any of the plaintiffs who have experienced credit or IRS irregularities have satisfied the remaining elements of the *Lujan* test and can overcome defendants' other arguments that jurisdiction is lacking.

c. Future Identity Theft and Other Future Harms

The CAC alleges generally that the defendants' actions "placed millions of government workers at a heightened risk of identity theft." CAC ¶ 210; *see also* NTEU Compl. ¶ 92. The CAC plaintiffs allege that as a group, they face an increased risk of experiencing a host of injuries, including: "money and time expended to prevent, detect, contest, and repair identity theft [and]

fraud;" "money and time expended to order credit reports and place temporary freezes on credit, and to investigate options for credit monitoring and identity theft protection services;" and "lost opportunity costs and loss of productivity from efforts to mitigate and address the adverse effects of the Data Breaches." CAC ¶ 163.

Numerous individual plaintiffs predicate injury in fact on the likelihood of possible harm in the future. For example:

- Plaintiff Myrna Brown provided sensitive information in an SF 86 form in connection with her employment with the Commerce Department, and she has received notice from OPM that her data was compromised. "Her exposure to the Data Breaches has caused Brown to review her financial accounts with greater frequency. Brown now also reviews her credit reports with greater frequency. Additionally, Brown suffers stress resulting from fear that the theft of her sensitive personal information will impair her ability to obtain future federal employment or security clearances, and fear for the safety of her family members who serve in the military. CAC ¶ 18.

- Plaintiff Maryann Hibbs "works as a Registered Nurse at the Veterans Health Administration, where she has been employed for approximately 23 years." Hibbs also previously served in the Army National Guard. Hibbs provided sensitive information to the federal government and received notice from OPM that such information has been compromised in the Data Breaches. Hibbs suffers stress resulting from concerns for her personal safety and that of her family members." CAC ¶ 35.

- Plaintiff Robert Slater, who currently serves in the Army, "suffers stress resulting from concerns that the theft of his sensitive personal information will impair his ability to obtain a higher security clearance, or future employment with a government contractor when he leaves the Army. His exposure to the Data Breaches has also caused Slater to review his financial accounts and credit reports with greater frequency to detect fraudulent activity. CAC ¶ 46.

Some plaintiffs claim to be suffering from stress now due to a fear of identity theft, physical harm, or some unspecified threat to their safety in the future, CAC ¶¶ 18–19, 22–25, 28, 30–31, 35, 37, 43–44, 46, 50; NTEU Compl. ¶ 94; and others point to expenses they incurred to

prevent or monitor future identity theft. CAC ¶¶ 17, 21, 25, 28, 34, 40, 41.[15] The Court holds that none of these allegations sets forth an injury in fact.

Future harm is neither concrete nor imminent for standing purposes unless it is "certainly impending," *Pub. Citizen, Inc.*, 489 F.3d at 1293, or it presents a "substantial risk." *Clapper*, 568 U.S. at 414, 422 & n.5. A harm that is "remote, speculative, conjectural, or hypothetical" will not suffice. *Pub. Citizen, Inc.*, 489 F.3d at 1293; *see also Clapper*, 568 U.S. at 422 ("[R]espondents lack Article III standing because they cannot demonstrate that the future injury they purportedly fear is certainly impending . . . ."); *Williams v. Lew*, 77 F. Supp. 3d 129, 132–33 (D.D.C. 2015) (plaintiffs' fears, which "rest[ed] on [a] hypothetical premise," did not provide standing because they were based on possible future injury, not a certainly impending one), *aff'd*, 819 F.3d 466, 474 (D.C. Cir. 2016) (holding that a court "cannot exercise jurisdiction based on 'worr[ies] and concern[s]' that lack a reasoned basis") (alterations in original).

The D.C. Circuit recently weighed in on this issue in *Attias v. CareFirst Inc.*, 865 F.3d 620 (D.C. Cir. 2017). Although plaintiffs take the position that the decision binds this Court to find that they have standing to pursue their action, *see* Class Pls.' Suppl. Submission, the Court is not persuaded that the holding covers this case. The Court of Appeals found in that data breach lawsuit that the plaintiffs' plausible allegation that they were subject to a substantial risk of identity theft was sufficient to satisfy the injury-in-fact element of the *Lujan* test, but it drew that conclusion, and found the allegation to be plausible, under circumstances that do not pertain here.

---

15 For some plaintiffs, the CAC describes a greater degree of attention paid to financial matters, but the allegations do not even go so far as to include the vague references to "stress" or increased concern. For example, with respect to plaintiff Ryan Bonner, the CAC alleges only that Bonner provided sensitive personal information and received notice that the information had been compromised, and that "his exposure to the Data Breaches has caused Bonner to review his credit reports and financial accounts with greater frequency." CAC ¶ 15; *see also* CAC ¶ 13–14, 16–17, 20–21, 26–27, 29, 32–34, 36, 38–42, 45, 47–49.

The *Attias* case arose out of a cyberattack on CareFirst, a health insurance company. After the data breach was reported, plaintiffs sued and predicated standing on an allegation that the breach had exposed them to a heightened risk of identity theft in the future. The district court concluded that the plaintiffs' theory of injury was "too speculative" to satisfy the requirement in *Clapper* that the harm be "clearly impending," and it dismissed the case for lack of subject matter jurisdiction. *Attias v. CareFirst, Inc.*, 199 F. Supp. 3d 193, 200 (D.D.C. 2016).

The Circuit Court reversed, stating that the Supreme Court had "clarified that a plaintiff can establish standing by satisfying *either* the 'certainly impending' test *or* the 'substantial risk' test," *Attias*, 865 F.3d at 626–27 (emphasis in original), citing *Susan B. Anthony List v. Driehaus*, 134 S. Ct. 2334, 2341 (2014) (an allegation of future injury may suffice if the "threatened injury is certainly impending" or there "is a substantial risk that the harm will occur"). It then zeroed in on the latter:

> Under our precedent, "the proper way to analyze an increased-risk-of-harm claim is to consider the ultimate alleged harm," which in this case, would be identity theft, "as the concrete and particularized injury and then to determine whether the increased risk of such harm makes injury to an individual citizen sufficiently 'imminent' for standing purposes."

Id. at 627, quoting *Food & Water Watch, Inc. v. Vilsack*, 808 F.3d 905, 915 (D.C. Cir. 2015). The Court explained that since "[n]obody doubts that identity theft, should it befall one of these plaintiffs, would constitute a concrete and particularized injury," the critical question for injury-in-fact purposes "is whether the complaint plausibly *alleges* that the plaintiffs now face a substantial risk of identity theft as a result of CareFirst's alleged negligence in the data breach." *Id.* (emphasis in original). In other words, if plaintiffs can allege that the risk of future harm is substantial, that satisfies the *Lujan* requirement that the injury be imminent.

The Court then combed through the complaint to identify the allegations that made the claim of an increased risk plausible, *id.* at 627–28, and it noted that the complaint alleged that

CareFirst collected and stored sensitive information including credit card and social security numbers.[16] *Id.* It then concluded that the risk was more substantial than the risk presented in *Clapper*. *Id.* at 629.[17] The Court observed that the feared harm in *Clapper* "could only occur through the happening of a series of contingent events, none of which was alleged to have occurred by the time of the lawsuit." *Id.* at 628, citing *Clapper*, 568 U.S. at 410–14. But it found that the CareFirst data breach presented a different situation:

> Here, by contrast, an unauthorized party has already accessed personally identifying data on CareFirst's servers, and it is much less speculative – at the very least, it is plausible – to infer that this party has both the intent and the ability to use that data for ill. As the Seventh Circuit asked, in another data breach case where the court found standing, "Why else would hackers break into a . . . database and steal consumers' private information? Presumably, the purpose of the hack is, sooner or later, to make fraudulent charges or assume those consumers' identities."

Id. at 628–29, citing *Remijas v. Neiman Marcus Grp.*, 794 F.3d 688, 693 (7th Cir. 2015). Based on that analysis, the Court of Appeals found:

> No long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm; a substantial risk of harm exists already, simply by virtue of the hack and the nature of the data that the plaintiffs allege was taken.

Attias, 865 F.3d at 629.

While the Court used broad language to announce its conclusion, its determination that the *Attias* allegations were sufficient cannot be separated from its repetition of the rhetorical question

---

16 The district court had based its ruling on the fact that the complaint did not expressly allege that social security or credit card numbers had been *stolen*, and it took into consideration the affidavit of the CareFirst IT Security Official who averred that the most sensitive data, such as social security and credit card numbers, was not included in the data breach. *Attias*, 199 F. Supp. 3d at 196 n.1, 198 n.3, 200–01.

17 The Court of Appeals also noted that the complaint alleged that the theft of the insureds' names, in combination with their birth dates and other subscriber information, created a risk of "medical identity theft" in which an imposter could obtain medical services in their names. *Attias*, 865 F.3d at 628.

posed in *Remijas* and the Seventh Circuit's answer. In other words, standing in *Attias* was predicated on the slender thread that one could fairly assume what the thieves meant to do with the stolen information. While drawing such an inference may have been logical in the case of a domestic crime directed at credit and financial information maintained by a retail establishment or a private health insurer, it is not necessarily logical here, and *Attias* supplies no other principle to follow.

Plaintiffs suggest that this case is "on all fours with the allegations in *Attias*," Class Pls.' Suppl. Submission at 3, but they fail to address the fact that *Attias*, and the case upon which it relies, *Remijas*, were predicated on the theft of credit card information, which the courts inferred could be utilized by the hackers themselves to perpetrate financial fraud. *Remijas*, 794 F.3d at 692–93; *see also Galaria v. Nationwide Mut. Ins. Co.*, 663 F. App'x. 384, 388 (6th Cir. 2016) (court drew reasonable inference that the domestic criminal theft of personal information from an insurance company was for the fraudulent purposes alleged in the complaint). Moreover, in *Remijas*, there was clear evidence that a large number of the particular credit card numbers that had been stolen had already actually been used. *Id.* at 690. As the district court in *Attias* pointed out:

> *Remijas* involved a data breach of Neiman Marcus's computer systems, which compromised customers' credit card information, social security numbers, and birth dates. Of the 350,000 credit cards whose information was potentially exposed, 9,200 "were known to have been used fraudulently." In other words, the hackers had clearly demonstrated that they had the means and the will either to abuse the information they accessed or to sell it to others who did so.

193 F. Supp. 3d at 200, quoting *Remijas*, 794 F.3d at 690 (citations omitted).

But those allegations are absent here, and the complaint does not allege anything that even comes close.

Plaintiffs have not plausibly alleged that the means to commit credit card or bank fraud were included in this breach, since there is no allegation that those account numbers are called for in the standard forms at issue or that they are provided in the course of background investigations. The CAC alleges in paragraph 144 that the personal information provided to OPM includes "information about financial accounts" and "financial and investment records," *see also* CAC ¶¶ 66, 146, and it states that job applications "include financial information." CAC ¶ 144. But no plaintiff who alleges that he or she suffered from financial fraud, such as the unauthorized use of a credit or debit card, alleges that the card numbers or accounts that were compromised had been supplied to OPM in a government form.

Moreover, a detailed review of the forms themselves, which are specifically referenced in the complaint, *see, e.g.*, CAC ¶¶ 66–70, reveals that they do not ask for account-identifying information. The SF 85, the standard Questionnaire for Non-Sensitive Positions, asks no questions whatsoever concerning finances beyond calling for the identification of present and former employers. *See* https://www.opm.gov/forms/pdf_fill/sf85.pdf.

The more detailed SF 86, the Questionnaire for National Security Positions, does not ask applicants for their active credit or debit card numbers. The form, which is 127-pages long, finally gets to the questions related to business dealings and personal finances on page 63. *See* https://www.opm.gov/forms/pdf_fill/sf86-non508.pdf. And of the many questions asked, only

two call for account numbers of any sort,[18] and those ask about judgments against the applicant for delinquencies, or loans or credit accounts that resulted in foreclosures or cancellations for default – in other words, account numbers that are particularly unlikely to be useful for the perpetration of credit card fraud. But there is no allegation in the complaint that any of the plaintiffs who experienced an unauthorized use of a credit or debit card had provided those particular numbers on the SF 86 or that those were the accounts that were misused.

It has been noted that criminals may use stolen personal information as a step in the process of creating false accounts or engaging in identity theft. *See SAIC*, 45 F. Supp. 3d at 32 ("a criminal could obtain some of a victim's personal information from a data breach and then go 'phishing' to get the rest"). But plaintiffs do not allege that this was the purpose of the cyberattacks, the facts do not suggest that it was, and this would be the classic example of the sort of chain of events

18 The SF 86 asks applicants to provide the following types of financial information:

Page 63: Foreign investments: type of investment, value, date acquired and sold
Page 73: Foreign business activities
Page 100: Whether alcohol or drug use has had a negative impact on finances
Page 106: Any filing for bankruptcy
Page 107: Financial problems due to gambling losses; any failure to pay taxes
Page 108: Whether the applicant has ever been subjected to discipline or required to undergo counseling for misuse of an employer's credit card, and whether he or she is currently using credit counseling services
Page 109: A question on this page asks if the applicant is delinquent in child support payments, or if there has been a judgment entered against him, including any obligations as a sole debtor, tax liens, or delinquencies on other debts, and in that situation, it directs the applicant filling out the form to identify the loan or account number involved.
Page 110: Similarly, a question on page 110 asks about any repossessions, loan foreclosures, loan defaults, debts sent to a collection agency, credit cards cancelled for default, or cards for which the applicant is more than 120 days delinquent, and those numbers are called for as well.

There are no additional questions in the form that seek financial information.

undertaken by a series of independent actors that is inconsistent with the imminence needed for standing.[19]

Also, while this ruling is not based on the original complaints that were consolidated and amended in this multidistrict litigation, the Court notes that many of the plaintiffs specifically alleged that the breaches were widely reported to have been perpetrated by the Chinese government.[20] This was also the conclusion set forth in the U.S. House of Representatives

19 This is why plaintiffs' reliance on *Khan v. Children's Nat'l Health Sys.*, 188 F. Supp. 3d 524 (D. Md. 2016) is misplaced. Plaintiffs argued in their opposition that "put[ting] forth facts that provide either (1) actual examples of the use of the fruits of the data breach for identity theft, even if involving other victims; or (2) a clear indication that the data breach was for the purpose of using the plaintiffs' personal data to engage in identity fraud" can satisfy the clearly impending or substantial risk standard. CAC Pls.' Opp. at 17, quoting *Khan*, 188 F. Supp. 3d at 532. But even if the *Khan* formulation controlled in this district, plaintiffs make neither showing here.

The complaints do not suggest that "the fruits of the data breach" were used for the alleged identity thefts because, as noted above, they do not allege that OPM or KeyPoint maintained the account numbers that were used improperly, nor do they allege that the government forms compromised in the breaches call for that information. The CAC states conclusorily that "[s]tolen federal job applications and investigation forms contain . . . financial records that include bank account and credit card information," CAC ¶ 146, but that allegation is belied by the forms themselves, and no individual plaintiff alleges that he or she provided a credit card, debit card, or bank account number. One individual NTEU plaintiff alleged that through the SF 85P and 86 "he disclosed or authorized the release to OPM of, among other information . . . financial information (including his investment accounts)," NTEU Compl. ¶ 6; another simply alleges that "financial information" was provided, NTEU Compl. ¶ 8; and the third individual plaintiff does not mention finances at all. NTEU Compl. ¶ 7. And both complaints are devoid of allegations that would provide "a clear indication that the data breach was for the purpose of using the plaintiffs' personal data to engage in identity fraud." *Khan*, 188 F. Supp. 3d at 532.

20 *See, e.g., Am. Fed'n of Gov't Emps. v. OPM*, Case No. 15-1015, Compl. [Dkt. # 1] ¶ 68; *Krippendorf v. OPM*, Case No. 15-1321, Compl. [Dkt. # 1] ¶¶ 61, 73; *Robbeloth v. OPM*, Case No. 15-1449, Compl. [Dkt. # 1] ¶¶ 63, 75; *Brown v. OPM*, Case No. 15-1564, Compl. [Dkt. # 1] ¶ 67; *Bonner v. OPM*, Case No. 15-1617, Compl. [Dkt. # 1] ¶¶ 3 n.4, 54 n.30 (citing press articles); *Waid v. OPM*, Case No. 15-1653, Compl. [Dkt. # 1] ¶¶ 63, 76; *Woo v. OPM*, Case No. 15-1752, Compl. [Dkt. # 1] ¶ 63; *Cavis v. OPM*, Case No. 15-1810, Compl. [Dkt. # 1] ¶¶ 63, 76; *Smith v. OPM*, Case No. 15-1835, Compl. [Dkt. # 1] ¶ 71; *Hobbs v. OPM*, Case No. 15-1927, Compl. [Dkt. # 1] ¶ 63; *Hanagan v. OPM*, Case No. 15-1933, Compl. [Dkt. # 1] ¶ 57; *Fleishell v. OPM*, Case No. 15-2089, Compl. [Dkt. # 1] ¶¶ 7, 81; *Golden v. OPM*, Case No. 16-1253, Compl. [Dkt. # 1] ¶ 80.

Committee on Oversight and Government Reform transmitting the result of a formal investigation into the OPM breach. *See* The OPM Data Breach: How the Gov't Jeopardized Our Nat'l Sec. for More than a Generation, Comm. on Oversight and Gov't Reform, U.S. House of Reps., 114th Congress, Sept. 7, 2016 ("Congressional Report"), at iii, vi, 157. And, while the administration may have been officially circumspect at the time, possibly in light of the classified nature of the information, the state-sponsored nature of the attack was discussed publicly by some individual knowledgeable federal officials. *See* Paul Coyer, *U.S. Gov't Data Breach Exemplifies China's Cyber Insecurities*, Forbes Mag., Jul. 19, 2015 ("The Obama White House has been careful to not formally name China as the perpetrator, yet private security firms which have long experience tracking Chinese cyber activities, Members of Congress who have been briefed by intelligence officials, and even James Clapper, the Director of National Intelligence, have all pointed to China as the likely source of the hacking."); Ellen Nakashima, *Chinese government has arrested hackers it says breached OPM database*, Wash. Post, Dec. 2, 2015. Also, it does not appear that the theory has been revised or abandoned since that time. *See* Devlin Barrett, *Chinese National Arrested for Allegedly Using Malware Linked to OPM Hack*, Wash. Post, Aug. 24, 2017. While a finding concerning the source of the breach is beyond the scope of this proceeding at this juncture, these

circumstances render the Court unable to rely upon the presumption that animated the *Attias* and *Remijas* decisions.[21]

So here, we do have a situation where a "long sequence of uncertain contingencies involving multiple independent actors has to occur before the plaintiffs in this case will suffer any harm," *Attias*, 865 F.3d at 629, and what is more, the nature of that harm is entirely undefined.

There is no question that plaintiffs have plausibly alleged that the building blocks of some forms of identity theft – social security numbers coupled with names, birthdates, and addresses – were included in the cache of information that was taken from OPM. But the Consolidated Amended Complaint does not point to any particular objective behind the breach beyond the claim that it was carried out to obtain sensitive data for an unspecified "improper use." CAC ¶¶ 7, 117, 128, 132. Neither complaint directly alleges, or marshals any facts that would support an inference, that those behind this attack are likely to use the information for credit card fraud or

---

21 These circumstances further differentiate this case from *Khan*, 188 F. Supp. 3d at 532. The hackers' goal has not been revealed, and there are no allegations that financial fraud or identity theft were the purpose behind the cyberattack.

Plaintiffs contend that they have shown injury in fact anyway because they allege that the breaches were "a targeted and malicious attack," and not an inadvertent part of an ordinary burglary such as the theft of the laptop in the *SAIC* case. CAC Pls.' Opp. at 17–18, citing *Pisciotta v. Old Nat. Bankcorp*, 499 F.3d 629, 632 (7th Cir. 2007); *Am. Fed'n Gov't Emps. v. Hawley*, 543 F. Supp. 2d 44, 45, 50–51 (D.D.C. 2008). But these non-binding cases were decided before *Clapper*, and the standing decisions did not turn whether the data theft was targeted or malicious, rather than inadvertent.

In *Pisciotta*, the Seventh Circuit did not rely on the nature of the hack when ruling that plaintiffs had standing; it simply disagreed with the line of cases requiring plaintiffs whose data has been compromised to experience a misuse of the data in order to state an injury in fact. 499 F.3d at 634. Similarly, the standing decision in *Hawley* did not turn on the nature of the theft of personal data. 543 F. Supp. 2d at 50. More importantly, these cases predate *Clapper*, which made clear that "[a]llegations of *possible* future injury are not sufficient." 568 U.S. at 409, quoting *Whitemore v. Arkansas*, 495 U.S. 149, 158 (1990) (emphasis added) (internal alterations and quotation marks omitted). In other words, the allegation that the breaches of OPM and KeyPoint were "targeted and malicious" does not eliminate the requirement that plaintiffs' potential harm be certainly impending or, at least, that the risk of harm be "substantial."

identify theft purposes, that they are likely to make it available to other criminals for that purpose, or that the breach has enabled other bad actors to have greater access to the information than they did before. The Court is not suggesting that the breach was insignificant, or that it did not or could not have a serious impact on national security, possibly in ways that could affect or compromise some of the individuals involved. *See* Congressional Report at vi. But there is little alleged to indicate that there is any risk of the particular harm being proposed as a basis for Article III standing – future identity theft – much less, that the risk is now "substantial" in the wake of the events at OPM.[22] The *Attias* Court based its decision on a particular cybercrime in a commercial setting – "the hack and the nature of the data that the plaintiffs allege was taken" – and it did not purport to address every data breach, including those that might be state-sponsored. Since the Court lacks the basis available in *Remijas* or *Attias* to "presume" that the purpose of *this* hack was to facilitate fraud or identity theft,[23] this case is more analogous to *Clapper*, and it is not plausible

22 Plaintiffs' allegations that they face some sort of increased risk are highly conclusory, *see* NTEU Compl. ¶ 92 ("The Defendant's reckless indifference to her obligations has put NTEU members, including Plaintiffs . . . and their families, friends, and other associates at substantial risk of identity theft, thereby subjecting them to financial peril and inconvenience."); and the CAC does not even allege that the threat is substantial. *See* CAC ¶ 7 (plaintiffs' information "remains subject to a continuing risk of additional exposure or theft as a consequence of OPM's ongoing failure to secure it"); CAC ¶ 163 ("As a result of Defendants' violations of law, Plaintiffs and Class members . . . have experienced and/or face an increased risk of experiencing . . . money and time expended to prevent, detect, contest, and repair identity theft, fraud and other unauthorized uses of [government investigation information]; . . . money and time expended to ameliorate the consequences of the filing of fraudulent income tax returns; . . . lost opportunity costs and loss of productivity . . . ."); CAC ¶ 210 ("Defendants' failure to protect the [government investigation information] of Plaintiffs and Class Members abridged their privacy rights . . . and placed millions of government workers at a heightened risk of identity theft, fraud, and other detrimental consequences.").

23 While the Court is bound to accept the factual allegations in the consolidated amended complaint as true, and to resolve any inferences in plaintiffs' favor, it is not required to draw inferences or "presume" circumstances that are not supported by the available public record – which was cited heavily in plaintiffs' own previous allegations – on the matter.

to infer that plaintiffs now face a substantial risk of identity theft based on the allegations in the complaint.

As for the plaintiffs who allege a risk of future bodily injury or express concerns for their personal safety, CAC ¶¶ 13, 18, 22–26, 35, 37, 43, 44, the complaint is devoid of allegations that would give rise to a plausible conclusion that the threat is clearly impending or that the risk became significant as a result of the breach.[24]

With respect to plaintiffs' purchases of credit monitoring and other services to avoid future identity theft, those expenditures also do not constitute an injury in fact either. CAC Pls.' Opp. at 15 (arguing that plaintiffs "reasonably paid to protect themselves" from future injury). It is well-established that incurring "certain costs as a reasonable reaction to a risk of harm" does not provide for injury if "the harm [plaintiffs] seek to avoid is not certainly impending. In other words, respondents cannot manufacture standing merely by inflicting harm on themselves based on their fears of hypothetical future harm that is not certainly impending." *Clapper*, 568 U.S. at 402; *Attias*, 865 F.3d at 629 ("To be sure, such self-imposed risk-mitigation costs, when 'incurred in response to a speculative threat,' do not fulfill the injury-in-fact requirement."), quoting *Clapper*, 568 U.S. at 416–17. Even an "objectively reasonable likelihood" of harm sufficient to engender some

24 Plaintiff Jane Doe II bases her injury on the fact that her spouse, an Assistant United States Attorney, submitted sensitive personal information that was compromised. She states that she "experiences significant stress from fear that the exposure of her and her family members' sensitive personal information will cause them to be targeted for retaliatory attacks and bodily harm." CAC ¶ 23. However, Jane Doe II also specifically alleges that her spouse is "responsible for prosecuting large-scale narcotics and money laundering cases, including cases against international drug cartels known to target prosecutors, law enforcement officials, and their families," and that he "has received multiple death threats throughout his career and was the subject of an assassination attempt." *Id*. While one cannot deny or minimize the dangers faced by many prosecutors, the complaint makes it clear that the risk arose from the nature of the lawyer's public position, and there is nothing stated that would give rise to an inference that the cyberattack has made the attorney substantially more vulnerable to those who would do him harm.

anxiety does not create standing. *SAIC*, 45 F. Supp. 3d at 26, citing *Clapper*, 568 U.S. at 415–16. Since the risk of identity theft was neither clearly impending nor substantial, plaintiffs' purchases of credit monitoring services do not constitute injury in fact because the risk they sought to prevent is too speculative.

In sum, the Court holds that only the two plaintiffs who alleged that they incurred expenses to rectify the actual fraud or identity theft they experienced, CAC ¶¶ 22, 41, have alleged injury in fact.

2. Causation

This does not end the standing analysis. Those plaintiffs, as well as any other plaintiffs who experienced some sort of identity theft event without an economic loss, lack standing because their alleged injuries are not "fairly traceable" to defendants' challenged actions. *Lujan*, 504 U.S. at 560. Plaintiffs maintain that all they need to allege to show causation is that defendants failed to secure their personal information, hackers stole it, and plaintiffs "consequently were subjected to actual and imminent harm." CAC Pls.' Opp. at 23 ("Nothing further is required at this point to show that the harm is plausibly traceable to Defendants' misconduct."). But the allegations in the complaint do not even rise to the level of "consequently" – plaintiffs repeatedly allege that the breach occurred and an unauthorized use of personal information occurred "thereafter." And while the short discussion of causation at the conclusion of the *Attias* decision may lend some support to plaintiffs' legal position, *see Attias*, 865 F.3d at 629, the Court finds that neither complaint plausibly alleges any connection between the OPM breaches and the claimed harm.

Plaintiffs allege that OPM's failures enabled unknown third parties not before the Court to access their personal information, and they also allege that in some instances, plaintiffs' personal information has been used improperly by unknown parties. As the district court pointed out in *Food & Water Watch v. EPA*:

> The Supreme Court has stated that "[w]hen the suit is one challenging the legality of government action or inaction . . . [and] a plaintiff's asserted injury arises from the government's allegedly unlawful regulation of someone else . . . it becomes the burden of the plaintiff to adduce facts showing that those choices have been or will be made in such a manner as to produce causation and permit redressability of injury."

5 F. Supp. 3d 62, 76 (D.D.C. 2013), quoting *Lujan* at 560–61; *see also Lujan*, 504 U.S. at 562 ("[W]hen the plaintiff is not himself the object of the government action or inaction he challenges, standing is not precluded, but it is ordinarily 'substantially more difficult to establish.'"), quoting *Allen*, 468 U.S. at 758; *Warth*, 422 U.S. at 505 (holding that plaintiffs must show that, absent the government's allegedly unlawful actions, "there is a substantial probability that they would [not be injured] and that, if the court affords the relief requested, the [injury] will be removed"). Applying these principles in the data breach context, courts in this district have held: "to demonstrate causation, plaintiffs must put forward facts showing that their injuries can be traced to the specific data incident of which they complain and not to any previous theft or data loss incident." *Welborn*, 218 F. Supp. 3d at 79. Plaintiffs do not satisfy this standard for either defendant.

It is true that in the *Attias* case, the D.C. Circuit concluded, "[b]ecause we assume, for purposes of the standing analysis, that plaintiffs will prevail on the merits of their claim that CareFirst failed to properly secure their data and thereby subjected them to a substantial risk of identity theft, we have little difficulty concluding that their injury in fact is fairly traceable to CareFirst." *Attias*, 865 F.3d at 629 (citation omitted). But the Court noted that the issue had not been briefed extensively, *id.*, and there are too many missing links in the chain for that statement to pertain here. As noted above, unlike in *Attias*, plaintiffs do not allege here that either defendant maintained the financial account information used in the alleged identity thefts. Furthermore, they do not allege any facts that plausibly connect the various isolated incidents of the misuse or

attempted misuse of plaintiffs' information to the breaches at issue here. *Cf. Remijas*, 794 F.3d at 692–95 (plaintiffs had standing in a data breach case involving the theft of department store credit card numbers when the stolen card numbers were used after the hack to make fraudulent charges).

"Generally, to prove that a data breach caused identity theft, the pleadings must include allegations of a nexus between the two instances beyond allegations of time and sequence." *Resnick v. AvMed, Inc.*, 693 F.3d 1317, 1326 (11th Cir. 2012). But allegations of time and sequence are all that plaintiffs provide here: they allege that the breaches occurred and that plaintiffs then learned of the identity theft. *See* CAC ¶ 16 ("Bos . . . received notice from OPM . . . . Bos thereafter learned that an unauthorized credit card account had been opened in his name."); CAC ¶ 30 (plaintiff provided personal information to the federal government, learned of the data breaches, and was "thereafter" informed of unauthorized charges on his debit card); [25] CAC ¶ 14 (plaintiff provided sensitive personal information to the federal government, learned his information has been compromised in the data breaches, and later learned of a false tax return using his and his wife's personal information); *see also* CAC ¶¶ 17, 19, 24, 26, 28–32, 38, 41, 49, 50; NTEU Compl. ¶¶ 66–72, 79–84 (alleging that NTEU plaintiffs submitted "inherently personal information" to OPM, were notified that they were affected by the data breaches announced on June 4 and June 12, 2015, and that plaintiff Gambardella had three fraudulent credit card charges and a fraudulent 2015 tax return filed in his name).[26] The *Attias* Court was able to point to

25 Some allegations do not even include the "thereafter," but simply state that the breach occurred and certain financial irregularities – for which dates are not always provided – also occurred. *See* CAC ¶ 13 ("Plaintiff Travis Arnold . . . received notice from OPM . . . . In May 2015, while reviewing his bank statement, Arnold discovered an unauthorized charge . . . ." And "[w]hile reviewing his credit report, Arnold also learned that between six and ten unauthorized inquiries regarding his credit had been made.").

26 The NTEU complaint does not allege that plaintiffs Howell or Ortino experienced actual identity theft. *See* NTEU Compl. ¶¶ 85–86.

allegations that customers gave CareFirst their credit card information, *Attias*, 865 F.3d at 628, but no plaintiff here has alleged that he provided a credit or debit card number on the SF 85 or SF 86.

Moreover, the events alleged to have occurred after the breach are separated across time and geography, and they follow no discernible pattern: there are a handful of false income tax returns mixed in with such occurrences as a debit card charge here, a charge to a PayPal account (which requires a password) there, several new credit inquiries, the creation of a new cellular phone account, and the cancellation of an account with a local utility. One cannot easily construct any kind of colorable theory that would link these events together, especially given the absence of evidence that the account numbers utilized here were ever provided to OPM. The Court therefore holds that these sets of allegations that two things happened in sequence are not sufficient to show causation.

In addition, to hold defendants accountable for plaintiffs' alleged injuries, the Court would have to presume that the vast majority of identity thefts plaintiffs experienced were not perpetrated by other criminals or were not the result of data breaches of other entities.[27] Such a presumption, with no factual predicate in the complaints besides allegations based on chronology, stretches the notion of traceability in this case beyond constitutional limits, particularly given how common identity theft is in the digital age. *See SAIC*, 45 F. Supp. 3d at 32 ("In a society where around 3.3% of the population will experience some form of identity theft – regardless of the source – it is not surprising that at least five people out of a group of 4.7 million happen to have experienced some form of credit or bank-account fraud."). This case is even more attenuated, even if you count all

27 *But see* NTEU Compl. ¶¶ 85–86.

twenty of the CAC plaintiffs alleging some form of fraud: 20 out of 21.5 million is 0.00009 percent.

In the end, plaintiffs can point to nothing that would begin to connect this hack to such random events as an unauthorized spending spree at Best Buy. *See* CAC ¶ 39. Since plaintiffs' allegations of fraudulent financial activity are based on pure speculation about the actions of a chain of unknown third-party wrongdoers who are not before the Court, they are insufficient to establish standing. *See Clapper*, 568 U.S. at 414 (expressing the Court's "usual reluctance to endorse standing theories that rest on speculation about the decisions of independent actors"). Plaintiffs have not satisfied their burden to adduce facts showing that the choices of third parties "have been or will be made in such manner" to show causation as to OPM or KeyPoint. *Lujan*, 504 U.S. at 562.

For all of these reasons, the Court holds that neither the CAC nor NTEU plaintiffs have Article III standing, and it will grant defendants' motions to dismiss for lack of subject matter jurisdiction pursuant to Rule 12(b)(1).

The Court recognizes, particularly in light of the recent decision in *Attias*, that standing is a very close and difficult question in this case. But there are other significant challenges to subject matter jurisdiction to contend with. Even if plaintiffs have standing, they must establish that there has been a waiver of sovereign immunity that would give the Court authority to hear a claim against the United States, and the bulk of the Privacy Act claims and the APA claim fail for that reason. Furthermore, as a government contractor, KeyPoint also enjoys sovereign immunity, and there is no applicable exception that would allow the lawsuit against the firm to go forward. And in the end, the few CAC plaintiffs who can invoke the Privacy Act fail to state a claim, the CAC

complaint fails to state a claim under the Little Tucker Act, and the NTEU plaintiffs fail to state a constitutional claim.

II. Plaintiffs' Claims Cannot Proceed.

A. Claims Against OPM

1. Plaintiffs' Privacy Act claims must be dismissed.

The CAC plaintiffs' first count against OPM alleges that the agency violated the Privacy Act. CAC ¶¶ 175–85. This act "regulate[s] the collection, maintenance, use, and dissemination of information" by federal agencies, Privacy Act of 1974, § 2(a)(5), 88 Stat. 1896 (codified at 5 U.S.C. § 552a), setting detailed requirements on how agencies should manage their records. 5 U.S.C. § 552a(e). It provides "civil relief to individuals aggrieved by failures on the Government's part to comply with [the Act's] requirements," *Doe v. Chao*, 540 U.S. at 618, when those failures "have an adverse effect on an individual." 5 U.S.C. § 552a(g)(1)(D). Under the Act, the United States is liable for "[a]ctual damages sustained by the individual as a result of" the agency's failure to comply if a court determines that an agency has "acted in a manner which was intentional or willful." 5 U.S.C. § 552a(g)(4)(A) (setting the minimum amount a plaintiff obtains at "no less than $1,000").

Plaintiffs assert that the agency "willfully and intentionally failed to comply with [the Federal Information Security Management Act]" which "adversely affected Plaintiffs and Class members." CAC ¶ 178. In doing so, they contend, OPM violated both the disclosure provision, CAC ¶ 183, and the safeguards provision, CAC ¶ 182, of the Privacy Act.

a. All but two CAC plaintiffs fail to plead actual damages, and therefore the Court lacks subject matter jurisdiction to hear their claims.

The term "actual damages" under the Act is "limited to proven pecuniary or economic harm." *FAA v. Cooper*, 566 U.S 284, 299 (2012); *see also Earle v. Holder*, No. 11-5280, 2012

WL 1450574, at *1 (D.C. Cir. Apr. 20, 2012) (unpublished) ("[B]ecause nothing in appellant's pleadings could be construed as alleging he sustained pecuniary loss as a result of the [defendant's] alleged Privacy Act violation, the district court correctly determined he was not entitled to damages.").

Reading the complaint in the light most favorable to plaintiffs, the Court finds that all but two plaintiffs fail to allege facts that support a plausible inference that they sustained actual damages within the meaning of the Act. Plaintiffs who allege unauthorized charges on their financial accounts do not allege any out-of-pocket or unreimbursed costs resulting from the thefts, *see* CAC ¶¶ 13, 19, 29, 30, 38, 41, 50, so they have not alleged "actual damages" within the meaning of the Act. Further, most plaintiffs alleging other forms of identity theft, such as fraudulent tax returns or the improper use of Social Security numbers, allege that they spent time, but not money, addressing these events. *See* CAC ¶ 13, 14, 16, 17, 21, 24, 26, 28, 29, 31, 32, 39, 45, 49, 50. The plaintiffs who alleged emotional distress arising from the breaches, *see*, *e.g.*, CAC ¶¶ 22, 41, do not allege "actual damages" under the Act. *Cooper*, 566 U.S at 299, 304. And those plaintiffs who purchased credit monitoring services or incurred other expenses to prevent future identity theft, CAC ¶¶ 17, 21, 25, 28, 34, 40, 41, have not suffered actual damages because expenditures undertaken voluntarily to prevent possible future harm do not constitute actual damages attributable to OPM. *See* 5 U.S.C. § 552a(g)(4); *Welborn*, 518 F. Supp. 3d 82 fn.2 (holding that the plaintiffs' decisions "to spend money on credit monitoring services to prevent potential future harm does not allege actual damages attributable to the [agency]" under the Privacy Act). Therefore, none of these plaintiffs has alleged facts that would support the waiver of sovereign immunity needed to give this Court jurisdiction to hear their claims.

The two plaintiffs who spent money to address actual identity theft did allege "actual damages" under the Act. *See* CAC ¶¶ 22, 41. But their disclosure provision claim fails under Rule 12(b)(6) because it does not plausibly allege that OPM "disclosed" private information as that statutory term has been defined by the D.C. Circuit, and their safeguards provision claim fails because they have not pled sufficient facts to allege that their injuries were "a result of" OPM's actions.

b. The disclosure provision claim fails because OPM did not intentionally or willfully disclose plaintiffs' information within the meaning of the Act.

Plaintiffs allege that OPM violated the disclosure provision of the Privacy Act. CAC ¶ 183. This provision prohibits a federal agency from disclosing "any record . . . contained in a system of records" without the written consent of the "individual to whom the record pertains." 5 U.S.C. § 552a(b). But this claim fails because it hinges on the act of third-party cyber criminals who hacked OPM's systems and were outside of OPM's control. CAC ¶¶ 114–37.

The D.C. Circuit has held, upon review of the Act's "purposes, legislative history, and integrated structure . . . that Congress intended the term 'disclose' to apply in virtually all instances to an agency's unauthorized transmission of a protected record, regardless of the recipient's prior familiarity with it." *Pilon v. U.S. Dep't of Justice*, 73 F.3d 1111, 1124 (D.C. Cir. 1996). In this case, OPM did not "transmit" plaintiffs' information: a third party stole it. *See also VA Data Theft Litig.*, 2007 WL 7621261, at *6 ("It is difficult to imagine how an illegal act of a third party over whom the [agency] had no control could . . . constitute an intentional or willful disclosure by the [agency]"). Accordingly, the Court holds that plaintiffs' allegations do not plead an intentional or willful "disclosure" by OPM.

c. While plaintiffs have alleged a willful violation of the safeguards provision of the Privacy Act, their claim fails because they do not allege sufficient facts to show that their injuries were "a result of" OPM's conduct.

Plaintiffs also contend that OPM violated the safeguards provision of the Act. CAC ¶ 182. This provision requires federal agencies to "establish appropriate administrative, technical, and physical safeguards" to protect agency records. 5 U.S.C. § 552a(e)(10). To be an "intentional or willful" violation of this provision of the Privacy Act, an agency's actions must be "greater than gross negligence." *Waters v. Thornburgh*, 888 F.2d 870, 875 (D.C. Cir. 1989), *abrogated on other grounds by Chao*, 540 U.S. at 618. Its actions must be "so 'patently egregious and unlawful' that anyone undertaking the conduct should have known it 'unlawful.'" *Laningham v. U.S. Navy*, 813 F.2d 1236, 1242 (D.C. Cir. 1987), quoting *Wisdom v. Dep't of Hous. & Urban Dev.*, 713 F.2d 422, 425 (8th Cir. 1983).

Courts have held that allegations that an agency has been warned "of recurring, systemic, and fundamental deficiencies in its information security . . . if proven, would support a finding that defendants were warned of the deficiencies in their information security but failed to establish proper safeguards." *Hawley*, 543 F. Supp. 2d at 52 (holding that allegations that the Office of Inspector General "repeatedly informed" the agency of problems with its information security pled "intentional and willful" conduct); *see also VA Data Theft Litig.*, 2007 WL 7621261, at *4–*5 (allegations that an agency had been "warned repeatedly of deficiencies in [its] information security and yet failed to do anything to establish proper safeguards" were sufficient to plead that the agency "acted with something greater than gross negligence").

Plaintiffs here allege that OPM was warned repeatedly by its Office of Inspector General that the agency's computer security was deficient. CAC ¶¶ 84–113 (alleging that OPM was warned of information security deficiencies, including that it "fail[ed] to implement or enforce multi-factor authentication," "failed to promptly patch or install security updates for its systems,"

"lacked a mature vulnerability scanning program to find and track the status of security weaknesses . . . and failed to continuously monitor the security controls of its software systems," and "failed to engage in appropriate oversight of its contractor-operated systems"). They also allege that its failure to correct these specific deficiencies identified by the Inspector General "enabled hackers to access and loot OPM's systems for nearly a year without being detected," CAC ¶ 134; that "inadequate patching of software systems contributed to the [breaches]," CAC ¶ 135; and that "OPM's failure to implement . . . tiered identity management controls for system administrators exposed hundreds of its sub-networks, instead of a single sub-network, to breach," and if it implemented such controls, "the intrusion would have been detected earlier and the cyber thieves prevented from accessing the entire OPM network." CAC ¶ 137. Assuming the truth of the allegations in the complaint, as required when resolving a motion to dismiss, the Court holds that these factual statements do allege that OPM acted in an "intentional or willful" manner. *See Hawley*, 543 F. Supp. 2d at 52.

But the allegations still fail to state a claim because they plead facts insufficient for the Court to plausibly infer that OPM's failure to comply with the safeguards provision "ha[d] an adverse effect" on plaintiffs, 5 U.S.C. § 552a(g)(1)(D), or that their damages are "as a result of" the agency's failures. 5 U.S.C. § 552a(g)(4)(A). *See, e.g., Lugo v. U.S. Dep't of Justice*, 214 F. Supp. 3d 32, 41 (D.D.C. 2016) (holding that plaintiffs must plead "a 'causal connection' between the agency violation and the adverse effect"), quoting *Doe v. Dep't of Justice*, 660 F. Supp. 3d 31, 49 (D.D.C. 2009).

The two plaintiffs who allege actual damages make only a temporal connection between the OPM breaches and their damages. *See* CAC ¶ 22 (alleging that plaintiff was notified of the breaches, that in August of 2015, the FBI informed her "that her [government investigation

information] had been acquired by the so-called Islamic State of Iraq and al-Sham," and that while reviewing her credit report at an unspecified time, she discovered accounts had been fraudulently opened in her name and she purchased credit repair services and a copy of her credit report); CAC ¶ 41 (alleging that plaintiff was notified of the breaches; in June of 2015, she learned of fraudulent activity related to her account with an electrical utility; "additionally," she learned of fraudulent purchases on her debit card and two credit cards; and she purchased credit monitoring and repair). For the same reasons that plaintiffs do not plead injuries traceable to OPM for standing purposes, these allegations of problems that arose after the breaches are insufficient to plausibly allege that OPM's actions "ha[d] an adverse effect" on them or that that their identify thefts were "a result of" the OPM's actions or the breaches. Plaintiffs do not allege that OPM obtained or stored the account numbers that were improperly used – neither complaint alleges that the government was in possession of anyone's debit card number. And the facts alleged, as well as public statements about the breaches, suggest the attacks were not made for the purpose of ringing up retail charges or defrauding the electric company. Thus, it is equally if not more possible that plaintiffs' damages were the result of other criminal activities unrelated to the OPM breaches, and plaintiffs fail to allege facts, as opposed to conclusions, that would tie them to OPM.

Therefore, the Court will dismiss the few claims under Privacy Act over which it arguably has jurisdiction for failure to state a claim under Federal Rule of Civil Procedure 12(b)(6).

2. Plaintiffs fail to state a claim under the Little Tucker Act.

CAC plaintiffs' second count alleges that OPM violated the Little Tucker Act, 28 U.S.C. § 1346. This act authorizes a "civil action or claim against the United States, not exceeding $10,000 in amount, founded . . . upon any express or implied contract with the United States." *Id.* § 1346(a)(2). But in this case, there is no contract.

Plaintiffs allege in connection with federal employment that, along with all class members who completed SF 85 and SF 86 forms, they were in a contractual relationship with OPM. CAC ¶ 192. The contractual claim is based on the fact that each form contains a statement advising job applicants that the information called for "will be protected from unauthorized disclosure." *See, e.g.*, SF 86 at 2. It also warns that the information "may be disclosed without your consent . . . as permitted by the Privacy Act [5 U.S.C. § 552a(b)], and by routine uses," and each form lists eleven permitted uses. CAC ¶¶ 68–69; *see, e.g.*, SF 86 at 2. Plaintiffs assert that they relied on their "reasonable expectation and understanding that OPM was agreeing to prevent the disclosure of such information to unauthorized third parties and/or for improper purposes," and that OPM breached this agreement. CAC ¶¶ 192–93.

The statements in these forms, however, do not create a contract between plaintiffs and OPM because a pre-existing legal duty cannot form the basis for a contract. *Allen v. United States*, 100 F.3d 133, 134 (Fed. Cir. 1996) ("Performance of a pre-existing legal duty is not consideration."), citing Restatement (Second) of Contracts § 73 (1981) ("Performance of a legal duty owed to a promisor which is neither doubtful nor the subject of honest dispute is not consideration[.]"); *Floyd v. United States*, 26 Cl. Ct. 889, 891 (1992) ("That which one is under a legal duty to do, cannot be the basis for a contractual promise."), *aff'd*, 996 F.2d 1237 (Fed. Cir. 1993); *Youngblood v. Vistronix, Inc.*, No. 05-21, 2006 WL 2092636, at *4 (D.D.C. July 27, 2006) ("It is a general maxim of contract law that a party cannot offer as consideration a duty that the party is already obligated to perform.").

Plaintiffs contend that defendants' reference to the Privacy Act obligations in the forms overlooks OPM's separate duty to protect submitting information "from unauthorized disclosure." CAC Pls.' Opp. at 106 (quoting forms and arguing "[t]his promise stands by itself" and "is not

defined by reference to the Privacy Act"). But the single sentence merely acknowledges OPM's obligation to handle the information on the forms in accordance with federal law.

In any event, plaintiffs fail to allege facts to support the plausible inference of a contract. There is no offer because government forms are not considered binding contracts. *See, e.g.*, *Chattler v. United States*, 632 F.3d 1324, 1330 (Fed. Cir. 2011) (holding that a passport applicant's completion of a form for faster processing is a request for such processing, not a promise by the government to do so). Further, there was no acceptance because no one authorized to bind the government entered into a contract with plaintiffs. *Stout Rd. Assocs., Inc. v. United States*, 80 Fed. Cl. 754, 756 (2008) ("Only government officials who possess a Contracting Officer's warrant are authorized to bind the United States to a contract."). And as already explained above, there is no consideration. *Allen*, 100 F.3d at 134; *Floyd*, 26 Cl. Ct. at 891 (language in a contract that is "essentially no more than a restatement of a pre-existing legal duty . . . cannot stand as consideration sufficient to support a return promise").

3. The Court lacks subject matter jurisdiction to hear plaintiffs' claim under the APA.

The third count in the Consolidated Amended Complaint seeks declaratory and injunctive relief under the APA for OPM's alleged violations of the Privacy Act and FISMA. CAC ¶ 198 (alleging that "OPM acted arbitrarily and capriciously, [and] abused its discretion" when it violated the Privacy Act, FISMA, and regulations and technical standards for data security). Plaintiffs allege a series of failures by OPM relating to the operation of its computer and software systems, both before its systems were breached and after. CAC ¶¶ 200, 202.

The APA may serve as the waiver of sovereign immunity for claims brought by an individual who "suffer[ed a] legal wrong because of agency action, or [was] adversely affected or aggrieved by agency action." 5 U.S.C. § 702. It cannot, however, be invoked when another statute

"expressly or impliedly forbids the relief which is sought." *Id.* The Privacy Act limits the injunctive relief available under the statute to an order that an agency correct inaccurate, incomplete, irrelevant, or untimely records, 5 U.S.C §§ 552a(g)(1)(A), (2)(A), or give individuals access to their records. *Id.* § 552a(g)(1)(B). No other forms of injunctive relief are available to plaintiffs for violations of the Act. *See Edison v. Dep't of Army*, 672 F.2d 840, 846–47 (11th Cir. 1982), citing *Parks v. IRS*, 618 F.2d 677, 683–84 (10th Cir. 1980); *Cell Assocs., Inc. v. Nat'l Insts. of Health*, 579 F.2d 1155, 1161–62 (9th Cir. 1978); *Houston v. U.S. Dep't of Treasury*, 494 F. Supp. 24, 29 (D.D.C. 1979). Given this, plaintiffs cannot invoke the APA to obtain injunctive relief that the Privacy Act forbids.[28]

Plaintiffs' assertions that OPM's violations of the FIMSA warrant judicial review under the APA are similarly unavailing. The APA provides for judicial review of all "final agency action for which there is no other adequate remedy in a court," 5 U.S.C. § 704, except when "statutes preclude judicial review" or the "agency action is committed to agency discretion by law." *Id.* § 701(a). FISMA requires federal agencies to comply with information "security standards and conduct annual, independent evaluations of their information security." *Trusted Integration, Inc. v. United States*, 679 F. Supp. 2d 70, 74 (D.D.C. 2010), citing 44 U.S.C. §§ 3543–45. Although the D.C. Circuit has not ruled on the issue, it has indicated that the choices an agency makes in carrying out its FISMA obligations are not subject to judicial review. *See Cobell v. Kempthorne*, 455 F.3d 301, 314 (D.C. Cir. 2006) ("Notably absent from FISMA is a role for the judicial branch. We are far from certain that courts would ever be able to review the choices an agency makes in

28 Counsel for the CAC plaintiffs cited no authority for his contention that "the Court, under the APA, has the power to enforce the obligations of the agency to take the necessary measures to protect . . . private information . . . [I]t's really the claim of last resort when there's no alternative from the perspective of the class members to vindicate those rights." Hr'g Tr. at 31.

carrying out its FISMA obligations."). The Court holds that OPM's actions in carrying out the statute's requirements is committed to the agency's discretion, and not subject to judicial review under the APA. *Welborn*, 218 F. Supp. 3d at 81 ("[E]ach agency head is delegated full discretion in determining how to achieve [FISMA's] goals, which removes it from APA review.").

4. The NTEU plaintiffs fail to state a constitutional claim.

The NTEU plaintiffs have brought just one claim on behalf of themselves and the NTEU members whose personal information was exposed by the breaches: that OPM violated their constitutional right to informational privacy. NTEU Compl. ¶¶ 95–98. The Court holds that the NTEU complaint fails to allege a legally cognizable constitutional claim.

Legal authority on the existence of a constitutional right to informational privacy is limited. The Supreme Court has addressed the matter in only three cases, and in those cases, it assumed – but did not expressly recognize – the existence of such a legal interest. *See NASA v. Nelson*, 562 U.S. 134, 138 (2011); *Nixon v. Adm'r of Gen. Servs.*, 433 U.S. 425, 457–65 (1977); *Whalen v. Roe*, 429 U.S. 589, 599–600, 605–06 (1977). Based on the assumption that the Constitution protects an individual's "interest in avoiding disclosure of personal matters," *NASA*, 562 U.S. at 138, quoting *Whalen*, 429 U.S. at 599; *Nixon*, 433 U.S. at 457, the Court has examined whether there are constitutional limits on the amount or type of information the government may collect from citizens in three different contexts.

In *Whalen*, the Supreme Court considered a challenge to a New York statute that required physicians and pharmacists to report prescription information for certain narcotics to the state health department, which would maintain the information in a centralized computer file. 429 U.S. at 593. The plaintiffs expressed a fear that the computerized data would be misused, and they claimed that the statute invaded a constitutionally protected "zone of privacy," which included an "individual interest in avoiding disclosure of personal matters" and an interest in the right to make

important individual decisions independently. *Id.* at 598–600. But the Court found that the New York program did not pose a threat to either interest. *Id.* In a "word about issues we have not decided," the Court observed that the government's right to collect and use private data for public purposes is "typically accompanied by a concomitant statutory or regulatory duty to avoid unwarranted disclosures," and "that in some circumstances, that duty arguably has its roots in the Constitution." *Id.* at 605. But since it found that the New York statute reflected "a proper concern with, and protection of, the individual's interest in privacy," and that no right or liberty protected by the Constitution had been invaded, the Court pointedly stated: "[w]e therefore need not, and do not, decide any question which might be presented by the unwarranted disclosure of accumulated private data whether intentional or unintentional or by a system that did not contain comparable security provisions." *Id.* at 605–06.

In *Nixon*, the Court rejected a constitutional challenge to the Presidential Recordings and Materials Preservation Act, 44 U.S.C. § 2111, which compelled the President to turn over his Presidential papers and recorded conversations for review, and which the President claimed would violate his constitutional right to privacy. 433 U.S. at 429, 434, 454–55, 459. Emphasizing that the statute "mandate[d] regulations . . . aimed at preventing undue dissemination of private materials," *id.* at 458, the Court concluded that the public interest in preserving the documents outweighed any expectation of privacy the former President may have had in the materials, *id.* at 465, and it rejected his claim without ruling on the question of whether the President had a valid constitutional interest in the first place. *Id.* at 457 ("We *may* agree with appellant that, at least when Government intervention is at stake, public officials, including the President, are not wholly without constitutionally protected privacy rights in matters of personal life unrelated to any acts done by them in their public capacity.") (emphasis added).

Finally, in *NASA*, the Court held that challenged portions of the federal government's standard background investigation did not violate any constitutional right to informational privacy, emphasizing that the Privacy Act "covers all information collected during the background-check process" and imposes obligations for nondisclosure and criminal liability for willful violations of those obligations. 562 U.S. at 148, 156 (noting that in the context of hiring federal employees, the government "has a much freer hand in dealing 'with citizen employees than it does when it brings its sovereign power to bear on citizens at large'") (citation omitted).

Faced with this lack of definitive guidance from the Supreme Court, the D.C. Circuit has simply assumed in cases involving the collection of information that keeping one's information private may have a constitutional dimension, and it has not gone on to resolve the issue. *See, e.g.*, *Franklin v. Dist. of Columbia*, 163 F.3d 625, 638–39 (D.C. Cir. 1998); *Am. Fed'n of Gov't Emps. v. Dep't of Hous. & Urban Dev.*, 118 F.3d 786, 795 (D.C. Cir. 1997); *Nat'l Fed'n of Fed. Emps. v. Greenberg*, 983 F.2d 286, 294–95 (D.C. Cir. 1993); *United Steelworkers of Am., AFL-CIO-CLC v. Marshall*, 647 F.2d 1189, 1240–41 (D.C. Cir. 1980). Indeed, the Court expressed "grave doubts as to the existence of a constitutional right of privacy in the nondisclosure of personal information." *Am. Fed'n of Gov't Emps.*, 118 F.3d at 791 ("Were we the first to confront the issue we would conclude with little difficulty that such a right does not exist."); *see also Greenberg*, 983 F.2d at 293–94 (expressing the view of two panel members that *Whalen* is ambiguous as to the right's existence).[29] But given the uncertainties surrounding the issue and the absence of any clear indication from the Supreme Court, the D.C. Circuit in the *American Federation* case declined to

29 *But see Am. Fed'n of Gov't Employees*, 118 F.3d at 792 (suggesting in dicta the existence of a constitutional right to privacy in personal information), citing *United States v. Hubbard*, 650 F.2d 293, 304–06 (D.C. Cir. 1980); *Doe v. Webster*, 606 F.2d 1226, 1238 n.49 (D.C. Cir. 1979); *Utz v. Cullinane*, 520 F.2d 467, 482 n.41 (D.C. Cir. 1975).

"enter the fray by concluding that there is no such constitutional right." 118 F.3d at 793. It found reaching the issue to be unnecessary since the governmental interest in obtaining the information were sufficiently weighty to justify the intrusions into agency employees' privacy that were challenged in that case. *Id.*

Given this reticence on the part of the higher courts, and the absence of binding precedent one way or the other, this Court also finds it prudent to avoid wading into the legal waters surrounding the existence or scope of any constitutional right to informational privacy in general when it is not necessary to do so. And it is not necessary here because the NTEU claim is asking the Court to recognize a constitutional violation that no court has even hinted might exist: that the assumed constitutional right to informational privacy would be violated not only when information is disclosed, but when a third party *steals* it. *See* NTEU Compl. ¶¶ 96–98; NTEU's Opp. at 25–44 (arguing that the government has an affirmative duty "grounded in the constitutional right to informational privacy" to safeguard plaintiffs' private data). In other words, even if an individual who completes an SF 85 or SF 86 has a constitutional right to privacy in the information he or she is being asked to provide, it is well-established that the government has the right to gather that information. And even if it might violate the Constitution for the government to then deliberately disclose the information,[30] there is no authority for the proposition that the Constitution gives rise to an affirmative duty – separate and apart from the statutory requirements enacted by Congress – to protect the information in any particular manner from the criminal acts of third parties. *See, e.g., Harris v. McRae*, 448 U.S. 297, 317–318 (1980) (discussing the Due Process Clause of Fifth

30 *See Eagle v. Morgan*, 88 F.3d 620 (8th Cir. 1996); *Sheets v. Salt Lake Cty.*, 45 F.3d 1383 (10th Cir. 1995); *James v. Douglas*, 941 F.2d 1539 (11th Cir. 1991); *Fadjo v. Coon*, 633 F.2d 1172 (5th Cir. 1981).

Amendment and declining to "translate the limitation on governmental power implicit in the Due Process Clause" into an affirmative obligation on the government).

At bottom, what the NTEU plaintiffs allege is a violation of the Privacy Act, *see* NTEU Compl. ¶ 97 ("By failing to heed the repeated warnings of OPM's OIG and otherwise failing to satisfy obligations imposed on her by statute and other appropriate authority, the Defendant has manifested reckless indifference to her obligation to safeguard personal information . . . ."), but they have not brought a Privacy Act claim or alleged the facts that would enable them to do so, and they cannot find support for the allegedly unfulfilled "obligation" in the Constitution.

The sole source plaintiffs identify for the existence of the affirmative duty they would have this Court enforce is a law review article. NTEU's Opp. at 37, citing A. Michael Froomkin, Government Data Breaches, 24 Berkley Tech. L. J. 1019, 1049 (2009) ("When the State takes a person's data and holds it in a fashion outside the person's control, the State has done to that data exactly what Chief Justice Rehnquist said was necessary to trigger Due Process Clause protection: it has 'by the affirmative exercise of its power' taken the data and 'so restrain[ed]' it that the original owner is unable to exert any control whatsoever over how the government stores or secures it. The government's 'affirmative duty to protect' the data 'arises . . . from the limitation which it has imposed on his freedom to act on his own behalf' to keep the data secure."). Given the absence of any binding precedent – or even any persuasive writing from other courts – that recognizes a

constitutionally based duty to safeguard personal information,[31] and the D.C. Circuit's expressed skepticism about the existence of a right to informational privacy in the first place, this Court is compelled to hold that plaintiffs have failed to state a constitutional claim.[32]

B. Claims Against KeyPoint

The CAC plaintiffs assert that KeyPoint is liable for negligence, negligent misrepresentation and concealment, invasion of privacy, breach of contract, violations of the Fair Credit Reporting Act, and various state statutes governing unfair and deceptive trade practices and data breaches. CAC ¶¶ 216–75. The Court holds that plaintiffs' claims against KeyPoint must be dismissed because the firm is immune from suit as a government contractor.

The Supreme Court has held that "government contractors obtain certain immunity in connection with work which they do pursuant to their contractual undertakings with the United States." *Campbell-Ewald Co. v. Gomez*, 136 S. Ct. 663, 672 (2016), quoting *Brady v. Roosevelt S.S. Co.*, 317 U.S. 575, 583 (1943). That immunity applies unless a contractor "violates . . . federal law and the Government's explicit instructions" or "ha[s] 'exceeded his authority' or the authority 'was not validly conferred.'" *Id.* at 672–73, quoting *Yearsley v. W.A. Ross. Constr. Co.*, 309 U.S. 18, 20–21 (1940) ("[A]uthority to carry out [a] project [is] validly conferred, that is, [when] what

31 Plaintiffs cite a number of cases from other circuit courts for the proposition that the existence of the constitutional zone of privacy "is firmly established." *See* NTEU's Opp. at 29, n.7, citing *Denius v. Dunlap*, 209 F.3d 944, 955–56 (7th Cir. 2000); *Eagle v. Morgan*, 88 F.3d 620, 625 (8th Cir. 1996); *Sheets v. Salt Lake Cty.*, 45 F.3d 1383, 1388 (10th Cir. 1995); *James v. Douglas*, 941 F.2d 1539, 1544 (11th Cir. 1991); *Woodland v. City of Houston*, 940 F.2d 134, 138 (5th Cir. 1991); *Walls v. Petersburg*, 895 F.2d 188, 192–95 (4th Cir. 1990); *Barry v. City of New York*, 712 F.2d 1554, 1558–64 (2d Cir. 1983); *United States v. Westinghouse Elec. Corp.*, 638 F.2d 570, 577–80 (3d Cir. 1980). But those cases do not hold that the constitutional right would be violated when a third party steals private information from the government.

32 Since the Court finds that the NTEU case should be dismissed under both Rule 12(b)(1) and Rule 12(b)(6), it does not reach the issue of sovereign immunity, which was addressed only briefly by the parties.

[is] done was within the constitutional power of Congress, there is no liability on the part of the contractor for executing [Congress's] will.").

There is no dispute that KeyPoint was acting pursuant to a valid contract with OPM. CAC ¶¶ 1, 123 (alleging that KeyPoint was acting pursuant to a contract with the United States at the time of the events underlying the complaint). So the question is whether the complaint plausibly alleges that KeyPoint violated federal law and OPM's explicit instructions or exceeded its authority under the contract. *Campbell-Ewald Co.*, 136 S. Ct. at 672–73, quoting *Brady*, 317 U.S. at 575.

1. KeyPoint has derivative immunity because it was a government contractor.

Plaintiffs argue that because KeyPoint "violated section 552a(e)(10) . . . [and] section 552a(b) of the Privacy Act," it is not protected by derivative government immunity. CAC Pls.' Opp. at 60–61. KeyPoint maintains that this argument does not provide a basis to abrogate its immunity because a contractor cannot violate the Privacy Act. KeyPoint Mem. at 20.

The Privacy Act imposes requirements on each "agency" that maintains a system of records, *see, e.g.*, 5 U.S.C. § 552a(d), and section 552a(a)(1) of the statute refers to 5 U.S.C. § 551, the Freedom of Information Act, for the definition of the term agency:

> "[A]gency" as defined in section 551(1) of this title includes any executive department, military department, Government corporation, Government controlled corporation, or other establishment in the executive branch of the Government (including the Executive Office of the President), or any independent regulatory agency . . . .

5 U.S.C. § 552(f)(1). With respect to government contractors, the statute expressly provides:

> When an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system.

5 U.S.C. § 552a(m)(1). Thus, the Act requires that the *agency* ensure that the requirements of the Act are implemented; it does not hold contractors responsible for doing so. *See Metro. Life Ins. Co. v. Blyther*, 964 F. Supp. 2d 61, 71 (D.D.C. 2013), citing *Unt v. Aerospace Corp.*, 765 F.2d 1440, 1447 (9th Cir. 1985) (dismissing Privacy Act claims against insurance companies that cover life insurance for federal employees and holding that "the Privacy Act does not apply to government contractors"); *see also Abdelfattah v. DHS*, 787 F.3d 524, 533 n.4 (D.C. Cir. 2015) ("[t]he Privacy Act creates a cause of action against only federal government agencies and not private corporations or individuals"); *see also Martinez v. Bureau of Prisons*, 444 F.3d 620, 624 (D.C. Cir. 2006) (holding that the Act "authoriz[es] suit against an 'agency'" and affirming dismissal of Privacy Act claims against individuals because individuals are not federal agencies).

2. Plaintiffs do not adequately identify a portion of KeyPoint's contract with OPM that KeyPoint breached.

Plaintiffs argue, though, that KeyPoint "breached the terms of its contract with OPM . . . [because] [f]ederal contracts necessarily incorporate the requirements of the Privacy Act" via section 552a(m)(1). CAC Pls.' Opp. at 61–62, citing CAC ¶ 123 ("The contract between OPM and KeyPoint incorporates the requirements of the Privacy Act. 5 U.S.C. § 552a(m)(1)").

But this is simply an attempt to do indirectly what plaintiffs cannot do directly, and it fails as well. It is true that section 552a(m)(1) provides: "[w]hen an agency provides by a contract for the operation by or on behalf of the agency of a system of records to accomplish an agency function, the agency shall, consistent with its authority, cause the requirements of this section to be applied to such system." 5 U.S.C. § 552a(m)(1); *see also* 48 C.F.R. § 24.102(a). But the implementing regulation goes on to provide: "the system of records operated under the contract is deemed to be maintained by the agency," 42 C.F.R. § 24.102(c), and section 552a(m)(1) makes

clear that the contractor and its employees shall be considered employees of the agency. So this provision does not supply a basis to transfer Privacy Act liability to KeyPoint.

Even if one can draw an inference that pursuant to this provision of the Act, OPM imposed contractual requirements that prohibited KeyPoint from "disclosing" any record in accordance with § 552a(b), and bound it to establish appropriate safeguards under § 552a(e)(1), the complaint does not allege facts that would show that these presumed contractual terms were violated. There is no allegation in the complaint that KeyPoint "disclosed" anything – the complaint alleges that KeyPoint was the victim of a breach, and that a set of its log-in credentials was "stolen." CAC ¶¶ 4, 117, 127, 133.

With respect to safeguards, plaintiffs conclusorily allege that KeyPoint breached its contract with OPM because it "fail[ed] to ensure the security and confidentiality of records and to protect against known and anticipated threats," CAC ¶ 123, and by "unreasonably failing to safeguard its security credentials and Plaintiffs' [government investigation information]." CAC ¶ 122. But these general statements do not supply any facts and do not state a claim for breach of contract. Plaintiffs allege that KeyPoint "lack[ed] software logs to track malware entering its systems and data exiting its systems," *id.* ¶ 121, but they can point to no provision of the contract between OPM and KeyPoint requiring those measures. A plaintiff must provide "factual content [in her complaint] that allows the court to draw the reasonable inference that the defendant is liable for the misconduct alleged," *Brown v. Sessoms*, 774 F.3d 1016, 1020 (D.C. Cir. 2014), quoting *Iqbal*, 556 U.S. at 678, and those facts are lacking here.

Finally, plaintiffs make only conclusory allegations that KeyPoint exceeded its authority in executing its contract with OPM. *See* CAC ¶ 122 (alleging that "[b]y unreasonably failing to safeguard its security credentials and Plaintiffs' and Class members' [government investigation

information], KeyPoint departed from its mandate, exceeded its authority, and breached its contract with OPM"). These allegations offer no more than "labels and conclusions" and so they do not suffice to state a claim. *Iqbal*, 556 U.S. at 678 (2009), quoting *Twombly*, 550 U.S. at 555.

3. Even if KeyPoint acted negligently, it did not lose its sovereign immunity.

Finally, plaintiffs maintain that "derivative sovereign immunity is not available to contractors who act negligently in performing their obligations under the contract." CAC Pls.' Opp. at 62, quoting *In re Fort Totten Metrorail Cases*, 895 F. Supp. 2d 48, 74 (D.D.C. 2012). But *Fort Totten* does not eliminate contractor immunity any time a plaintiff alleges negligence by government contractor.

Applying the doctrine of derivative immunity for government contractors for the first time in this circuit, *Fort Totten* involved a claim against a subcontractor that had agreed to replace certain safety features on train tracks and conduct safety tests of those features. 895 F. Supp. 2d at 72–73. The plaintiffs asserted that the subcontractor "negligently failed to perform safety and compatibility testing in violation of its contractual obligations and applicable standards of care," but the contractor asserted it had derivative sovereign immunity under *Yearsley*. *Id.* at 74–75. The purported sovereign entity, Washington Metropolitan Area Transit Authority ("WMATA"), filed cross-claims against the subcontractor for breach of contract and negligence. *Id.* at 75.

In deciding whether the subcontractor had immunity, the court analyzed the various claims against the subcontractor, considering whether they were predicated on the subcontractor carrying out its contract with WMATA or on the subcontractor's breach of that contract and negligence in performing its obligations under the contract. *Id.* WMATA asserted that the subcontractor was required by the contract to ensure the compatibility of certain products to perform the requisite safety testing but failed to carry out these obligations. *Id.* Thus, the court concluded, "the very premise of these claims is that [the contractor] acted *against* the 'will of the sovereign' by

breaching its contractual duties to [the sovereign entity] and by performing negligently under the contract," undermining the contractor's attempt to invoke derivative immunity. *Id.* The court held that the contractor was "not entitled to derivative sovereign immunity under *Yearsley* as to these claims." *Id.*

The instant case is distinguishable from *Fort Totten*, which involved the unique circumstance where the governmental entity itself was making the allegation. Here, plaintiffs provide only conclusory allegations that KeyPoint exceeded its authority or acted negligently, and its conclusory allegations are based on its contentions that KeyPoint violated FISMA and breached its contract with OPM. *See* CAC ¶¶ 122–24. But as explained above, plaintiffs do not identify any contract provisions that KeyPoint allegedly violated, and their claims that it violated federal law cannot stand. And importantly, the sovereign in this case, OPM, does not disavow the actions of KeyPoint. Indeed, the complaint indicates as much, alleging that "OPM did not terminate or suspend its contract with KeyPoint." CAC ¶ 5. Thus, plaintiffs fail to plead facts sufficient to allege that KeyPoint violated OPM's explicit instructions or exceeded its authority under its contract with the agency.[33]

33 Plaintiffs also cite *Worcester v. HCA Management Co.*, 753 F. Supp. 31 (D. Mass. 1990), to support their argument that KeyPoint does not have derivative sovereign immunity, but that case is inapplicable. *Worcester* holds that, in addition to the exceptions recognized in *Campbell-Ewald*, a separate exception exists "when a private corporation who performs governmental duties pursuant to contractual authority from the government is sued for negligence in the performance of the[] duties." 753 F. Supp. at 38. The court relied on *Brady v. Roosevelt*, which held that a contractor cannot "escape liability for a negligent exercise of . . . delegated power," 317 U.S. at 583, because "the government is not the 'real party in interest'" when the contractor acts negligently. *Worcester*, 753 F. Supp. at 38, quoting *Brady*, 317 U.S. at 584. But *Brady* concerned "whether respondent can escape liability for a negligent exercise of . . . delegated power if we assume that by contract it will be exonerated or indemnified [by the federal government]." *Brady*, 317 U.S. at 583–84. Since KeyPoint will not be indemnified by the federal government in this case, *Brady* is not directly applicable, and *Worcester* is not binding on this Court in any event.

Accordingly, all of plaintiffs' claims against KeyPoint will be dismissed for lack of subject matter jurisdiction.

C. Claims against both defendants for declaratory judgment and injunctive relief will be dismissed for lack of subject matter jurisdiction.

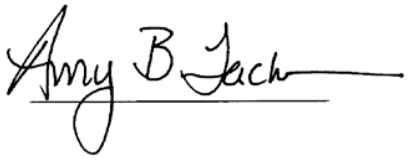
Finally, the Court will dismiss the CAC plaintiffs' Count IV, which seeks a declaration that defendants' conduct is unlawful, a judgment requiring them to indemnify plaintiffs for their economic injury and provide "free lifetime identity theft protection services," and an order that OPM implement a data security plan that complies with the Privacy Act and FISMA. CAC ¶¶ 208–15. They assert that equitable relief is warranted under the APA, the Declaratory Judgment Act, the common laws and statutory provisions that KeyPoint violated, and the Court's inherent authority. CAC ¶ 209.[34] But, as explained above, the APA does not provide relief for plaintiffs' claims. Also, as explained above, neither the Privacy Act, the Little Tucker Act, nor the APA provide plaintiffs the relief they seek, and the United States may not be sued without a waiver of sovereign immunity. *United States v. Mitchell*, 463 U.S. 206, 212 (1983). Finally, the Declaratory Judgment Act does not provide a private right of action or an independent source of federal jurisdiction, *see*, *e.g.*, *Ali v. Rumsfeld*, 649 F.3d 762, 778 (D.C. Cir. 2011). Accordingly, the Court also dismisses Count IV of the CAC.

CONCLUSION

For the reasons set forth above, the Court will dismiss plaintiffs' Consolidated Amended Complaint and the NTEU Complaint for lack of subject matter jurisdiction based on both standing and sovereign immunity grounds, and the Court also finds that the CAC fails to state a claim under

34 Characterizing their request for relief for indemnity from economic harm as seeking "equitable relief" does not allow plaintiffs to circumvent the Privacy Act's requirement that they suffer actual damages to obtain relief under the Act, *Cooper*, 132 S. Ct. at 1453, nor does it allow plaintiffs to circumvent the APA's prohibition against monetary damages. 5 U.S.C. § 702 (providing for judicial review of claims "seeking relief other than money damages").

the Privacy Act and the Little Tucker Act, and that the NTEU complaint fails to state a constitutional claim. A separate order will issue.



AMY BERMAN JACKSON
United States District Judge

DATE: September 19, 2017

IN THE UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN RE U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY LITIGATION This Document Relates To: *NTEU v. McGettigan*, 15-cv-1808-ABJ (D.D.C.) 3:15-cv-03144 (N.D. Cal.)	Misc. Action No. 15-1394 MDL Docket No. 2664

NOTICE OF APPEAL

Notice is given this 19th day of September, 2017, that Plaintiffs National Treasury Employees Union (NTEU), Eugene Gambardella, Stephen Howell, and Jonathon Ortino (collectively, NTEU Plaintiffs) hereby appeal to the United States Court of Appeals for the District of Columbia Circuit from the judgment of this Court entered on the 19th day of September, 2017, in favor of Defendant Kathleen McGettigan, Acting Director, Office of Personnel Management, against NTEU Plaintiffs.[1]

[1] Pursuant to Federal Rule of Civil Procedure 25(d), when a public officer who is a party in an official capacity ceases to hold office, the officer's successor is automatically substituted as a party, and later proceedings should be in the substituted party's name. Accordingly, Kathleen McGettigan has been substituted for her predecessor.

Respectfully submitted,

Gregory O'Duden
Larry J. Adkins

/s/Paras N. Shah
Paras N. Shah
Allison C. Giles
NATIONAL TREASURY EMPLOYEES UNION
1750 H Street, N.W.
Washington, D.C. 20006
Tel: (202) 572-5500
Email: greg.oduden@nteu.org
Email: larry.adkins@nteu.org
Email: paras.shah@nteu.org
Email: allie.giles@nteu.org

Counsel for NTEU Plaintiffs

September 19, 2017

CLERK: Please mail copies of the above Notice of Appeal to the following at the address indicated:

ELIZABETH J. SHAPIRO
ANDREW E. CARMICHAEL
JOSEPH BORSON
U.S. Department of Justice
Civil Division, Federal Programs Branch
20 Massachusetts Avenue, NW, Room 7218
Washington, DC 20530

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN RE: U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION	Misc. Action No. 15-1394 (ABJ) MDL Docket No. 2664
This Document Relates To: ALL CASES	

NOTICE OF APPEAL

Notice is hereby given that the Class Plaintiffs—i.e., each and every plaintiff included in the Consolidated Amended Complaint [Dkt. # 63]—appeal to the United States Court of Appeals for the District of Columbia Circuit from the Order granting Defendant KeyPoint Government Solutions, Inc.'s Motion to Dismiss Plaintiffs' Consolidated Amended Complaint and granting Federal Defendants' Motion to Dismiss the Consolidated Amended Complaint [Dkt. # 116], and the accompanying Memorandum Opinion [Dkt. # 117], entered on September 19, 2017. With respect to the Federal Defendants, Class Plaintiffs appeal from the District Court's dismissal of the First Claim for Relief of the Consolidated Amended Complaint, but not the dismissal of the Second, Third, and Fourth Claims for Relief.

DATED: October 5, 2017

Respectfully submitted,

GIRARD GIBBS LLP

By: /s/ *Daniel C. Girard*
Daniel C. Girard

Daniel C. Girard
Jordan Elias
601 California Street, 14th Floor
San Francisco, CA 94108
Phone: (415) 981-4800
Facsimile: (415) 981-4846
Email: dcg@girardgibbs.com

Interim Lead Class Counsel

David H. Thompson
Peter A. Patterson
COOPER & KIRK, PLLC
1523 New Hampshire Avenue, N.W.
Washington, D.C. 20036

Tina Wolfson
AHDOOT & WOLFSON, PC
1016 Palm Avenue
West Hollywood, CA 90069

John Yanchunis
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 North Franklin Street, 7th Floor
Tampa, FL 33602

Plaintiffs' Steering Committee

Gary E. Mason
WHITFIELD BRYSON & MASON LLP
5101 Wisconsin Ave., NW.
Suite 305
Washington, D.C. 20016

Liaison Counsel

CERTIFICATE OF SERVICE

I hereby certify that on October 5, 2017, I filed the above document with the Court's CM/ECF system, which will send notice of such filing to all parties.

/s/ *Daniel C. Girard*
Daniel C. Girard

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN RE: U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION	Misc. Action No. 15-1394 (ABJ) MDL Docket No. 2664
This Document Relates To: ALL CASES	

SUPPLEMENT TO NOTICE OF APPEAL

Class Plaintiffs hereby supplement their notice of appeal filed October 5, 2017 [Dkt. #120] to provide a complete list of plaintiffs who are party to this appeal.

The Class Plaintiffs are: American Federation of Government Employees, AFL-CIO; Travis Arnold; Tony Bachtell; Ryan Bonner; Monty Bos; Gardell Branch; Myrna Brown; Heather Burnett-Rick; Robert Crawford; Paul Daly; Jane Doe; Jane Doe II; John Doe; John Doe II; John Doe III; Michael Ebert; Kelly Flynn; Alia Fuli; Johnny Gonzalez; Lillian Gonzalez-Colon; Orin Griffith; Jennifer Gum; Michael Hanagan; Maryann Hibbs; Deborah Hoffman; Michael Johnson; Cynthia King-Myers; Ryan Lozar; Teresa J. McGarry; Charlene Oliver; Toralf Peters; Mario Sampedro; Timothy Sebert; Zachary Sharper; Robert Slater; Darren Strickland; Peter Uliano; Nancy Wheatley; and Kimberly Winsor.

DATED: October 11, 2017

Respectfully submitted,

GIRARD GIBBS LLP

By: /s/ *Daniel C. Girard*

Daniel C. Girard
Jordan Elias
601 California Street, 14th Floor
San Francisco, CA 94108
Phone: (415) 981-4800
Facsimile: (415) 981-4846
Email: dcg@girardgibbs.com

Interim Lead Class Counsel

David H. Thompson
Peter A. Patterson
COOPER & KIRK, PLLC
1523 New Hampshire Avenue, N.W.
Washington, D.C. 20036

Tina Wolfson
AHDOOT & WOLFSON, PC
1016 Palm Avenue
West Hollywood, CA 90069

John Yanchunis
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 North Franklin Street, 7th Floor
Tampa, FL 33602

Plaintiffs' Steering Committee

Gary E. Mason
WHITFIELD BRYSON & MASON LLP
5101 Wisconsin Ave., NW.
Suite 305
Washington, D.C. 20016

Liaison Counsel

CERTIFICATE OF SERVICE

I hereby certify that on October 11, 2017, I filed the above document with the Court's CM/ECF system, which will send notice of such filing to all parties.

/s/ *Daniel C. Girard*
Daniel C. Girard

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF COLUMBIA

IN RE: U.S. OFFICE OF PERSONNEL MANAGEMENT DATA SECURITY BREACH LITIGATION	Misc. Action No. 15-1394 (ABJ) MDL Docket No. 2664
This Document Relates To: ALL CASES	

NOTICE OF APPEAL

The Class Plaintiffs hereby give notice of a protective appeal to the United States Court of Appeals for the Federal Circuit. Class Plaintiffs previously noticed an appeal to the United States Court of Appeals for the District of Columbia Circuit, which has been docketed in that court under case number 17-5232.

This Notice of Appeal is filed solely for the purpose of preserving Class Plaintiffs' rights in the event that the Court of Appeals for the District of Columbia Circuit holds that appellate jurisdiction lies exclusively in the Federal Circuit under 28 U.S.C. § 1295(a)(2). Class Plaintiffs intend to seek an immediate stay of this protective appeal in the Federal Circuit, and counsel for Defendants have indicated that they will not oppose the stay motion.

The Class Plaintiffs giving notice of this protective appeal are the American Federation of Government Employees, AFL-CIO; Travis Arnold; Tony Bachtell; Ryan Bonner; Monty Bos; Gardell Branch; Myrna Brown; Heather Burnett-Rick; Robert Crawford; Paul Daly; Jane Doe; Jane Doe II; John Doe; John Doe II; John Doe III; Michael Ebert; Kelly Flynn; Alia Fuli; Johnny

Gonzalez; Lillian Gonzalez-Colon; Orin Griffith; Jennifer Gum; Michael Hanagan; Maryann Hibbs; Deborah Hoffman; Michael Johnson; Cynthia King-Myers; Ryan Lozar; Teresa J. McGarry; Charlene Oliver; Toralf Peters; Mario Sampedro; Timothy Sebert; Zachary Sharper; Robert Slater; Darren Strickland; Peter Uliano; Nancy Wheatley; and Kimberly Winsor.

The judgment, order, or part thereof being appealed are the Order granting Defendant KeyPoint Government Solutions, Inc.'s Motion to Dismiss Plaintiffs' Consolidated Amended Complaint and granting Federal Defendants' Motion to Dismiss the Consolidated Amended Complaint [Dkt. # 116], and the accompanying Memorandum Opinion [Dkt. # 117], entered on September 19, 2017. With respect to Federal Defendants, Class Plaintiffs appeal from the District Court's dismissal of the First Claim for Relief of the Consolidated Amended Complaint, but not the dismissal of the Second, Third, and Fourth Claims for Relief.

DATED: November 8, 2017

Respectfully submitted,

GIRARD GIBBS LLP

By: /s/ *Daniel C. Girard*
Daniel C. Girard

Daniel C. Girard
Jordan Elias
601 California Street, 14th Floor
San Francisco, CA 94108
Phone: (415) 981-4800
Facsimile: (415) 981-4846
Email: dcg@girardgibbs.com

Interim Lead Class Counsel

David H. Thompson
Peter A. Patterson
COOPER & KIRK, PLLC
1523 New Hampshire Avenue, N.W.
Washington, D.C. 20036

Tina Wolfson
AHDOOT & WOLFSON, PC
1016 Palm Avenue
West Hollywood, CA 90069

John Yanchunis
MORGAN & MORGAN COMPLEX LITIGATION GROUP
201 North Franklin Street, 7th Floor
Tampa, FL 33602

Plaintiffs' Steering Committee

Gary E. Mason
WHITFIELD BRYSON & MASON LLP
5101 Wisconsin Ave., NW.
Suite 305
Washington, D.C. 20016

Liaison Counsel

CERTIFICATE OF SERVICE

I hereby certify that on November 8, 2017, I filed the above document with the Court's CM/ECF system, which will send notice of such filing to all parties.

/s/ *Daniel C. Girard*
Daniel C. Girard

CERTIFICATE OF SERVICE

I hereby certify that on May 10, 2018, I electronically filed the foregoing with the Clerk of the Court for the United States Court of Appeals for the District of Columbia Circuit, via the appellate CM/ECF system. Case participants who are registered CM/ECF users will be served by the appellate CM/ECF system.

Dated: May 10, 2018

/s/ *Jordan Elias*

Counsel for Class Plaintiffs–Appellants