Exhibit 4

FILED
2010 Apr-21 PM 03:15
U.S. DISTRICT COURT
N.D. OF ALABAMA

IN THE UNITED STATES DISTRICT COURT
NORTHERN DISTRICT OF ALABAMA
SOUTHERN DIVISION

JIM HENRY PERKINS and JESSIE FRANK QUALLS, on their own behalf and on the behalf of all others similarly situated,

Plaintiffs,

v. **CV No. 2:07-310-IPJ**

UNITED STATES DEPARTMENT OF VETERANS AFFAIRS; et al.

Defendants.

MEMORANDUM OPINION

This case is before the court upon remand from the Eleventh Circuit to conduct a "claim-by-claim" analysis to determine the validity of plaintiffs' remaining challenges brought under the Administrative Procedures Act ("APA"), 5 U.S.C. § 551 *et seq.*, and seeking to enforce provisions of the Privacy Act, 5 U.S.C. § 552a; the E-Government Act of 2002, 44 U.S.C. § 3501 note; and the Veterans Benefits, Health Care, and Information Technology Act of 2006, 38 U.S.C. § 5724. Only counts two, five, six, and eight remain, and the court examines each claim in turn.

Factual Background

On January 22, 2007, an employee of the U.S. Department of Veterans

Affairs ("VA") reported an external hard drive containing personally identifiable information and individually identifiable health information of over 250,000 veterans was missing from the Birmingham, Alabama Medical Center's Research Enhancement Award Program ("REAP"). VA Office of Inspector General ("OIG") Report, at 7. The IT Specialist responsible for the external hard drive, "John Doe," used the hard drive to back up data on his computer and other data from a shared network drive.[1] The hard drive is thought to contain the names, addresses, social security numbers ("SSN"), dates of birth, phone numbers, and medical files of hundreds of thousands of veterans and also information on more than 1.3 million medical providers. VA OIG Report at 7, 9 (doc. 33-2). To date, it has not been recovered.

John Doe was an IT Specialist working for the Birmingham REAP, a program that focused on "changing the practices of health care providers to ensure that they provide the latest evidence-based treatment, and on using VA databases

---

[1]The REAP Director approved the purchase of external hard drives as a means to provide more space to the Medical Center's near-full server. VA OIG Report, at 15. No policy required the protection of sensitive data on removable computer storage devices unless such devices were to be carried outside a VA facility. *Id.* at 16. The REAP Director claimed the Information Security Officer ("ISO") conferred with him in making the decision to purchase the external hard drives, but the ISO claimed he was not involved and did not know of the need for additional server space. The VA OIG concluded no one made a timely request to the ISO for additional space. VA OIG Report, at 15.

to link the care of VA patients to more general information on the population as a whole." *Id.* at 3. To reach these goals, the Birmingham REAP collects data on patients and medical providers from multiple sources for dozens of separate research projects." *Id.* The Data Unit of the Birmingham REAP was comprised of the Data Unit Manager, three IT Specialists, and two student program support Assistants. *Id.* at 4. John Doe worked "with national VA databases and design[ed] statistical programs to support Birmingham REAP research projects." *Id.*

The VA OIG identified three projects for which John Doe was conducting research. The first "involved developing a set of performance measures for diabetes management, specifically aimed at intensifying medication to improve glucose levels, cholesterol, and blood pressure"; the second "involved examining the quality of care to patients following myocardial infarction . . ., and attempted to determine whether certain demographic characteristics of the medical providers, such as their age, impacted the care rendered to these patients"; and the third "involved using a patient survey to identify use of over-the-counter medications in patients taking prescription medications and link the information obtained to various VA databases to determine whether patients suffered any adverse effects from the combination of medications." *Id.* at 22, 25, 30. In gathering the information needed to complete these projects, John Doe improperly received

access to various databases and stores of information, and various components of the VA improperly released information to John Doe or gave John Doe such access. *Id.* at 22-33. He was therefore able "to accumulate and store vast amounts of individually identifiable health information that was beyond the scope of the projects he was working on. [The OIG] believe[s] much of this information was stored on the missing external hard drive." *Id.* at 22. Accurate reporting of what information was on the external hard drive has been difficult because the hard drive is still missing; John Doe encrypted or deleted multiple files from his computer after reporting the data missing; and John Doe was not initially forthright with criminal investigators. *Id.* at ii.

After John Doe reported the missing hard drive on January 22, 2007, the VA Security Operations Center ("SOC") was immediately notified. *Id.* at 7. The SOC wrote a report and provided it to the VA OIG on January 23, 2007; on that same day, an OIG criminal investigator came to the Birmingham VAMC and conducted an interview. The Federal Bureau of Investigation became involved in the investigation on January 24, 2007. A forensic analysis of John Doe's computer began on January 29, 2007, and on February 1, 2007, the OIG began to analyze what data could have been on the missing hard drive. *Id.* at 8, 9. Press releases dated on February 2 and 10, 2007, discussed the loss of the hard drive and the information it contained.

> Subsequent to the reported loss of the Birmingham REAP data but prior to receiving the results of the OIG analysis of this data on February 7, 2007, VA senior management concluded that anyone whose SSN was thought to be contained in any of the missing files, irrespective of the ability of anyone possessing this data to match an SSN with a name or any other personal identifier, should be notified and offered credit protection. The basis for this decision was a memorandum issued on November 7, 2006. . . . The memorandum states that "in the event of a data loss involving individual and personal information. . . VA officials have a responsibility to notify the individual(s) of the loss in a timely manner and to offer these protection services."

Id. at 11. The VA sent letters to those individuals whose information was thought to be compromised by the data breach, which gave them the option of one year of free credit monitoring services. *Id.* at 12.

The VA had also requested the Department of Health and Human Services to perform a risk analysis focusing on the Centers for Medicaid and Medicare Services ("CMS") data involved in the breach. *Id.* The missing external hard drive contained approximately 1.3 million health care providers' information,

including the SSNs of 664,165 health care providers. *Id.* On March 28, 2007, the CMS Chief Information Officer and Director sent a letter to the VA Assistant Secretary for Office of Information and Technology that stated, based on the CMS's completed independent risk analysis:

> [T]here is a high risk that the loss of personally identifiable information may result in harm to the individuals concerned. The letter requested that "VA immediately take appropriate countermeasures to mitigate any risk of harm, including notifying affected individuals in writing and offering free credit monitoring to individuals whose personal information may have been contained on the file."

Id. From April 17 to May 22, 2007, the VA sent notification letters to the 1.3 million health care providers. *Id.* By May 31, 2007, it sent additional letters offering one year of credit monitoring to the 664,165 health care providers whose SSNs appeared to be on the hard drive. VA OIG Report, at 12.

Analysis

A valid claim under the APA must attack agency action, which is defined as "includ[ing] the whole or a part of an agency rule, order, license, sanction, relief or the equivalent or denial thereof, or failure to act." *Fanin v. U.S. Dep't of*

Veterans Aff., 572 F.3d 868, 877 (11th Cir. 2009) (citing 5 U.S.C. § 551(13)).

> If the claim attacks an agency's action, instead of failure to act, and the statute allegedly violated does not provide a private right of action, then the "agency action" must also be a "final agency action." [5 U.S.C. § 704; *see also Norton v. S. Utah Wilderness Alliance*, 542 U.S. 55, 61-62, 124 S.Ct. 2373, 2379 (2004)]. "To be considered 'final,' an agency's action: (1) must mark the consummation of the agency's decisionmaking process–it must not be of a merely tentative or interlocutory nature; and (2) must be one by which rights or obligations have been determined, or from which legal consequences will flow. *U.S. Steel Corp. v. Astrue*, 495 F.3d 1272, 1280 (11th Cir. 2007)(quoting *Bennett v. Spear*, 520 U.S. 154, 177-78, 117 S.Ct. 1154, 1168 (1997)).

Id. However, if the claim challenges a failure to act, the court may compel "agency action unlawfully withheld or unreasonably delayed. . . only where a plaintiff asserts that an agency failed to take a *discrete* agency action that it is *required* to take." *Id.* at 877-878 (citing *Norton*, 542 U.S. at 64) (emphasis in original).

Further, the court notes the remaining claims seek only injunctive and

declaratory relief. Such relief may be granted only if the plaintiffs demonstrate that they are "likely to suffer future injury." *City of Los Angeles v. Lyons*, 461 U.S. 95, 105, 103 S.Ct. 1660, 1667 (1983); *Lujan v. Defenders of Wildlife*, 504 U.S. 555, 564, 112 S.Ct. 2130, 2138 (1992) (citing *Lyons*, 461 U.S. at 102) ("'Past exposure to illegal conduct does not in itself show a present case or controversy regarding injunctive relief.'"); *Seigel v. LePore*, 234 F.3d 1163, 1176-77 (11th Cir. 2000) (*en banc*) ("As we have emphasized on many occasions, the asserted irreparable injury "must be neither remote nor speculative, but actual and imminent.") (citations omitted). *Emory v. Peeler*, 756 F.2d 1547, 1552 (11th Cir. 1985) (To grant declaratory relief, "there must be a substantial continuing controversy between parties having adverse legal interests. The plaintiff must allege facts from which the continuation of the dispute may be reasonably inferred. Additionally, the continuing controversy . . . must be real and immediate, and create a definite, rather than speculative threat of future injury.").

Count Two

The plaintiffs claim that the VA failed "to create and maintain an accounting of the date, nature, and purpose of its disclosures" pursuant to the Privacy Act, 5 U.S.C. § 552a(c)(1), when John Doe accessed VA files to complete

VA projects. Joint Status Report ("JSR"), at 8 (doc. 56). The Privacy Act requires

> [e]ach agency, with respect to each system of records under its control, shall–
>
> (1) except for disclosures made under subsections (b)(1) or (b)(2) of this section, keep an accurate accounting of–
>
> (A) the date, nature, and purpose of each disclosure of a record to any person or to another agency made under subsection (b) of this section; and
>
> (B) the name and address of the person or agency to whom the disclosure is made. . .

5 U.S.C. § 552a(c)(1). Under the exception provided in subsection (b)(1), agencies need not provide an accounting for disclosures made to "officers and employees of the agency which maintains the record who have a need for the record in the performance of their duties." 5 U.S.C. § 552a(b)(1). Accordingly, to the extent John Doe needed the information that he accessed to perform his duties, the VA had no obligation to account.

To the extent John Doe had no need for the information contained on the external hard drive in the performance of his duties, the plaintiffs must show the disclosure was pursuant to one of the provisions in 5 U.S.C. § 552a(b)(3)-(12).

See 5 U.S.C. § 552a(c)(1)(A). After failing to argue in the JSR that any of those subsections apply, plaintiffs now claim that the VA's disclosure to John Doe falls under 5 U.S.C. § 552a(b)(5), which requires accounting when the disclosure is "to a recipient who has provided the agency with advance adequate written assurance that the record will be used solely as a statistical research or reporting record, and the record is to be transferred in a form that is not individually identifiable."

However, the accounting requirement in 5 U.S.C. § 552a(b)(5) is not triggered by the activity at issue in this case. An accounting is required only upon a disclosure to a recipient described in that subsection. Although "recipient" is not defined in the Privacy Act, it does not stand to reason that an agency that maintains records needed by one of its own researchers to fulfill his duties would be required to provide *itself* with "advance adequate written assurance that the record will be used solely as a statistical research or reporting record." Indeed, pertinent legislative history and Office of Management and Budget ("OMB") regulations suggest that an accounting was only intended when the disclosures were to individuals or agencies outside the agency maintaining the record. *See* S. REP. NO. 93-1183 (1974) *reprinted in* U.S. CODE CONGRESSIONAL AND ADMINISTRATIVE NEWS, 6916, 6967 (stating that subsection 201(b)(4) "[r]equires any federal agency that maintains a personal information system or file to maintain an accurate accounting of the date, nature, and purpose of nonregular access

granted to the system, and each disclosure of personal information made to any person *outside the agency, or to another agency*. . . .") (emphasis added); H.R. No. 93-1416, 2 (describing the summary and purpose of the Act as "requir[ing] agencies to keep an accounting of transfers of personal records *to other agencies and outsiders*"); 40 Fed. Reg. 28955 (July 9, 1975) (differentiating between "agencies disclosing records" and "recipient agencies" in the context of 5 U.S.C. § 552a(b)(5)).

Even if subsection (b)(5) is applicable in this case, the plaintiffs argue only that John Doe gave an advance adequate written assurance before accessing information from only one database, the Veterans Integrated Service Network ("VISN") 7 Data Warehouse. Plaintiff's Response (doc. 64) at 4. Accordingly, subsection (b)(5) applies only for John Doe's access to the VISN 7 Data Warehouse to perform research for "Project 1," which involved diabetes management research. *See* VA OIG Report, at 22. Moreover, the plaintiffs cannot show that any failure to account for John Doe's access to the VISN 7 Data Warehouse to research diabetes management is causing them harm. Although the plaintiffs are upset about the loss of their personal information and the prospect of potential credit fraud in the future, any accompanying harm is attributable to the

loss of the information in the first place, *not* the purported failure to account.[2] Thus, even assuming *arguendo* that 5 U.S.C. § 552a(b)(5) applies, the plaintiffs cannot show that the alleged harm is fairly traceable to the VA's conduct, a deficiency fatal to their claim. *See Allen v. Wright*, 468 U.S. 737, 753 & n.19, 104 S.Ct. 3315, 3325 & n.19 (1984) (plaintiffs do not have standing where they failed to allege injuries that are caused by the defendants).

Because of these sufficient and independent reasons, the plaintiffs have not shown that the VA failed to take discrete agency action that it was required to take. Accordingly, the court finds that the plaintiffs have failed to state a claim upon which relief can be granted, and Count Two is due to be **DISMISSED**.

---

[2]The plaintiffs urge, "The Veterans have a right to know what information [was on the hard drive]. They deserve to know the 'purpose' for which John Doe was using the information," Plaintiff's Response, at 8 (doc. 64). However, the VA OIG report details, to the extent determinable, the information on the hard drive and the purpose for which John Doe was accessing the information. The VA OIG Report states that the hard drive is believed to contain "personally identifiable information and/or individually identifiable health information for over 250,000 veterans, and information obtained from the [CMS], on over 1.3 million medical providers." VA OIG Report, at i. Moreover, it was difficult for the VA to make such a determination, as John Doe was not candid when he was interviewed; he deleted or encrypted files from his computer after the hard drive went missing; and he tried to hide the extent, magnitude, and impact of the missing data. *Id.* at ii. Lastly, the plaintiffs know that the purpose John Doe was accessing the VISN 7 Data Warehouse was related to his research for "Project 1," *id.* at 22-23, which "involved developing a set of performance measures for diabetes management, specifically aimed at intensifying medication to improve glucose levels, cholesterol, and blood pressure," VA OIG Report, at 22.

Count Five

Count Five involves the VA's alleged failure to establish appropriate safeguards in violation of the Privacy Act, 5 U.S.C. § 552a(e)(10). The plaintiffs have failed to argue that the alleged conduct of the VA constituted a failure of discrete agency action that the VA was required to take, but request that Count Five "move forward as detailed in the Plaintiffs' Statement in the Joint Report." Plaintiff's Brief, at 13 (doc. 64). In the Joint Status Report, the plaintiffs devote just over one page to briefing this issue and cite 5 U.S.C. § 552a(e)(10),[3] arguing that the VA failed to enforce this subsection in the numerous ways listed in their complaint.[4] Joint Status Report ("JSR"), at 10-11 (doc. 56). The plaintiffs then

[3]5 U.S.C. § 552a(e)(10) requires the VA to "establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained."

[4]Plaintiffs cite specifically to paragraph 80 of the Second Amended Complaint (doc. 21), which states:

> Among other things, Defendants' failures include operating a computer system or database from which an employee, including John Doe, can download or copy information, like the Personal Information and the Medical Information, onto the VA External Hard Drive without proper encryption and when not necessary to perform his or her duties; failing to conduct a data access inventory for John Doe and other VA employees and contractors with access to the VA's office at the Pickwick Conference Center; failing to provide software that would require or enable encryption of data downloaded or copied

ask the court for an injunction forcing full implementation and compliance "with Handbook 6500 and other procedures and policies put in place in Birmingham by the VA in response to this incident, to conduct an independent audit of its compliance, and to file that audit with the court." Plaintiff's Response, at 14 (doc. 64) (footnotes added). Such an injunction is untenable.

Handbook 6500 is a seventy-one page (seven appendices excluded) document that details the responsibilities of almost two dozen information security personnel and dozens of policies and procedures. As pointed out by the defense, policies explained in the Handbook include maintaining the temperature in the building and proper use of the facsimile machines. In addition, the "other procedures and policies" put in place at the Birmingham facility are also

---

> to mobile hard drives and devices, like the VA External Hard Drive from VA computers and databases at the VA offices and facilities in the Birmingham, Alabama area; failing to secure the VA External Hard Drive under lock and key when not in the immediate vicinity of John Doe; failing to house and protect the VA External Hard Drive to reduce the opportunities for unauthorized access, use, or removal; failing to provide intrusion detection systems at the VA office at the Pickwick Conference Center; failing to store the VA External Hard Drive in a secure area that requires proper escorting for access; failing to require and conduct appropriate background checks on all VA employees and contractors with access to the VA Office in the Pickwick Conference Center; and failing to protect against the alienation and relinquishment of control over the VA External Hard Drive, causing the Personal Information and Medical Information to be exposed to unidentified third parties.

Second Amended Complaint (doc. 21), ¶ 80.

numerous. *See e.g.*, VA Directive 6504 (doc. 61-3) (governing the transmission, transportation and use of, and access to, VA data outside VA facilities); VA Handbook 6500, at 7 (doc. 61-4) (a seventy-one page document "establish[ing] the foundation for VA's comprehensive information security program and its practices that will protect the confidentiality, integrity, and availability of information"); Medical Center Memo 00-ISO-02 (doc. 61-5) ("assign[ing] responsibility and establish[ing] procedures for managing computer files at the Birmingham VA Medical Center"); Medical Center Memo 00-ISO-05 (doc. 61-6) (requiring VA employees at the Medical Center to get permission before use of removable storage media, especially Universal Serial Bus ("USB") devices, and requiring written permission for the removal of sensitive information from VA facilities); Information Security Program VISN 7 AIS Operational Security Policy (doc. 61-9) (establishing procedures to implement a "structured program to safeguard all IT assets"); Memorandum 10N7-077 of VISN 7 VA Southeast Network (doc. 61-10) (stating "It is the policy of VISN 7 that no sensitive information ([personal health information or personal identifiable information]) will be stored on the storage media of any device without encryption or where the device is not *physically secured* to prevent accidental loss of sensitive information in the event of theft") (emphasis in original).

Cases that suggest a broad injunction enforcing all of these policies is

appropriate are "relic[s] of a time when the federal judiciary thought that structural injunctions taking control of executive functions were sensible. That time has past." *Rahman v. Chertoff*, 530 F.3d 622, 626 (7th Cir. 2008). "The limitation to discrete agency action precludes the kind of broad programmatic attack [the Supreme Court] rejected in *Lujan v. National Wildlife Federation*, 497 U.S. 871, 110 S.Ct 3177, 111 L.Ed.2d 695 (1990)." *Norton v. S. Utah Wilderness Alliance*, 542 U.S. 55, 64, 124 S.Ct. 2373, 2379-2380 (2004); *see Lujan*, 497 U.S. at 891 When presented with similar circumstances in *Lujan*, the Supreme Court responded:

> Respondent alleges that violation of the law is rampant within this program-failure to revise land plans in proper fashion, failure to submit certain recommendations to Congress, failure to consider multiple use, inordinate focus upon mineral exploitation, failure to provide required public notice, failure to provide adequate environmental impact statements. Perhaps so. But respondent cannot seek *wholesale* improvement of this program by court decree, rather than in the office of the Department or the halls of Congress, where programmatic improvements are normally made.

Lujan, 497 U.S. at 891. Courts are not empowered to compel "compliance with

broad statutory mandates," *Norton*, 542 U.S. at 66-67, nor can they engage in general review of an agency's day-to-day operations to ensure such compliance. *Id.*; *Lujan*, 497 U.S. at 899.

Even if this court could pass on such a generalized challenge, the court is convinced that Count Five is moot.

> "'[A] case is moot when the issues presented are no longer "live" or the parties lack a legally cognizable interest in the outcome.' " *County of Los Angeles v. Davis,* 440 U.S. 625, 631, 99 S.Ct. 1379, 59 L.Ed.2d 642 (1979) (quoting *Powell v. McCormack,* 395 U.S. 486, 496, 89 S.Ct. 1944, 23 L.Ed.2d 491 (1969)). The underlying concern is that, when the challenged conduct ceases such that " 'there is no reasonable expectation that the wrong will be repeated,' " *United States v. W.T. Grant Co.,* 345 U.S. 629, 633, 73 S.Ct. 894, 97 L.Ed. 1303 (1953), then it becomes impossible for the court to grant " 'any effectual relief whatever' to [the] prevailing party," *Church of Scientology of Cal. v. United States,* 506 U.S. 9, 12, 113 S.Ct. 447, 121 L.Ed.2d 313 (1992) (quoting *Mills v. Green,* 159 U.S. 651, 653, 16 S.Ct. 132, 40 L.Ed. 293 (1895)).

City of Erie v. Pap's A.M., 529 U.S. 277, 287, 120 S.Ct. 1382, 1390 (2000).

Because the evidence submitted to the court shows that new security procedures and policies have been implemented and the deficiencies revealed in the VA OIG Report have been remedied, there is no "live" issue for which this court can grant effectual relief.

Count Six

In Count Six, the plaintiffs claim that the VA failed to perform a privacy impact assessment ("PIA") pursuant to the E-Government Act of 2002 when it procured the external hard drives. Pursuant to the E-Government Act, agencies must perform a PIA before "developing or procuring information technology that collects, maintains, or disseminates information that is in an identifiable form." 44 U.S.C. § 3501 note (E-Government Act of 2002, § 208(b)(1)(A)). The definition of "information technology" includes "any equipment or interconnected system . . . used in the automatic acquisition, storage, analysis, evaluation, manipulation, management, movement, control, display, switching, interchange, transmission, or reception of data or information by the executive agency, if the equipment is used by the executive agency directly . . . ." 40 U.S.C. § 11101(6); *see* 44 U.S.C. § 3501 note, § 201 (applying definitions from 44 U.S.C. §§ 3502, 3601); 44 US.C. § 3502(9) (applying the definition of 40 U.S.C. § 11101(6)). The disputed issue is whether the purchase of the external hard drives triggered the duty to perform a PIA.

The plaintiffs claim that the inclusion of "any equipment" in the definition of information technology brings the hard drives within the meaning of the term, thereby requiring the PIA. However, such an interpretation is implausible, as it would require government agencies that maintain personal information on individuals to conduct or update a PIA each time it purchases any computer, monitor, router, telephone, calculator, or other piece of equipment involved in a system that stores, analyzes, or manages the data. Rather, the purchase of several external hard drives, seems to be a "minor change[] to a system or collection that do[es] not create new privacy risks," and therefore does not require a PIA. *See* M-03-22, Attachment A 2.B.3.g., Office and Management and Budget ("OMB") Guidance Implementing the Privacy Provisions of the E-Government Act of 2002, at Section II.B.3.f (doc. 61-15) (hereinafter "M-03-22").

Lending support to this interpretation is the fact that PIAs are required to address (1) what information is collected and why, (2) the agency's intended use of the information, (3) with whom the information would be shared, (4) what opportunities the veterans would have to decline to provide information or to decline to share the information, (5) how the information would be secured, and (6) whether a system of records is being created. *See* 44 U.S.C. § 3501 note (E-Government Act of 2002, § 208(b)(2)(B)); M-03-22, at Section II.C.1.a. These types of inquiries are certainly appropriate and required when the VA initially

created the Birmingham VAMC system and began collecting data, but not where already collected and stored data is simply being transferred from a server to an external hard drive. The factors above are not relevant for such a transfer and a new PIA would not be informative of what information is being collected, the intended use of the information, or with whom the information would be shared. Under such circumstances, Congress surely did not intend a PIA to be performed.

To the extent the plaintiffs argue that security procedures were not followed or hardware security protocols were breached at the VA facility in Birmingham when the external hard drive went missing, such claims are not actionable under the E-Government Act of 2002. Rather, those arguments should have been pursued pursuant to the Federal Information Security Management Act (FISMA), 44 U.S.C. §§ 3541 *et seq*., a claim that the plaintiffs waived after not pursuing it on appeal. *Fanin v. U.S. Dep't of Veterans Affairs*, 572 F.3d 868, 876 n.1.

Count 8

The final count before the court involves the VA's alleged failure to perform an independent risk analysis ("IRA") to determine the risk presented by the loss of the hard drive pursuant to the Veterans Benefits, Health Care, and Information Technology Act of 2006 (VBHCITA), 38 U.S.C. § 5724(a)(1). The plaintiffs also claim that the VA acted unreasonably by providing only one year of credit monitoring services.

The VBHCITA[5] provides:

> In the event of a data breach with respect to sensitive personal information that is processed or maintained by the Secretary, the Secretary shall ensure that, as soon as possible after the data breach, a non-Department entity or the Office of Inspector General of the Department conducts an independent risk analysis of the data breach to determine the level of risk associated with the data breach for the potential misuse of any sensitive personal information involved in the data breach.

38 U.S.C. § 5724(a)(1).

After John Doe reported the missing hard drive on January 22, 2007, the VA launched an immediate investigation that culminated in the decision to offer one year of free credit monitoring services for 198,760 living individuals whose information was contained on the hard drive. VA OIG Report, at 12. The VA made this decision *before* the completion of the IRA conducted by the Centers for Medicaid & Medicare Services ("CMS"). On February 7, 2007, VA senior

[5]The VBHCITA became effective December 22, 2006. The data breach incident at issue occurred on January 22, 2007. The VA passed regulations that became effective June 22, 2007, six months after the passage of the VBHCITA and five months after the loss of the external hard drive.

management decided that anyone whose SSN was on the hard drive should be notified and offered credit protection. *Id.* at 11. Approximately one and one-half months later, on March 28, 2007, the CMS Chief Information Officer and Director stated that based on the IRA, "There is a high risk that the loss of personally identifiable information may result in harm to the individuals concerned." *Id.* at 12. He recommended that the "VA immediately take appropriate countermeasures to mitigate any risk of harm, including notifying affected individuals in writing and offering free credit monitoring to individuals whose personal information may have been contained on the file." *Id.* Notification letters were sent out to the health care providers by May 31, 2007. *Id.*

Thus, the VA proactively assumed that the veterans were at risk and provided the remedy provided in the statute[6] *before* it had confirmation from the IRA that such a remedy was appropriate under the circumstances. By presuming a reasonable risk of harm from the disclosure of personally identifiable information and providing credit protection services required when an IRA reveals a "reasonable risk" of harm, *see* 38 U.S.C. § 5724(a)(2), the VA has provided the

[6]In addition, VA regulations limit credit monitoring awarded to those who are subject to a reasonable risk for misuse of sensitive personal information to one year. 38 C.F.R. § 75.118(a).

plaintiffs with any relief they are due.[7] Indeed, the IRA conducted by CMS affirmed the propriety of the relief offered by the VA.

Despite having been given such relief, the plaintiffs insist the IRA was insufficient and urge an additional IRA focusing on the veterans must be completed. However, the statute does not require an *individual* risk analysis as the plaintiffs state in their JSR, *See* JSR, at 12-13, 15, only an *independent* risk analysis.[8] The VA OIG Report contains multiple groups of individuals whose private information was compromised: veterans, VA OIG Report, at 7; physicians, *id.* at 10; deceased physicians, *id.*; other health care providers, *id.*; non-veteran, non-VA employees, *id.* at 24; and VA employees, *id.* Furthermore, some veterans were only identified by their SSNs; others were identified by SSNs and dates of birth; others by their name, SSN, and medical information; and others identified

---

[7] The plaintiffs offer a General Accountability Office report that states that a May 5, 2006, incident involving a missing tape with sensitive information of thousands of individuals on it warranted "credit protection and data breach analysis for 2 years." JSR, at 14. As the plaintiffs explain, however, only one year of credit protection was offered, while two years of breach analysis was given. Declaration of Michael Hogan ("Hogan Decl."), ¶¶ 2 (doc. 61-19) and Attachment A (doc. 61-20).

[8] The plaintiffs' argument that the CMS was an inappropriate entity to perform the IRA has no merit, as the statute requires either the VA OIG or a non-Department [of Veterans Affairs] entity to conduct the IRA. 38 U.S.C. § 5724(a)(1). The CMS is under the purview of the Department of Health and Human Services.

by various combinations of seven fields of identifying information. *Id.* at 9. The health care providers are identified on the hard drive by different combinations of forty-eight different fields of data. *Id.* at 10. All of this information was on a single external hard drive lost during a single data breach. The statute only requires an "independent risk analysis of the data breach," not multiple IRAs for each group of individuals whose information was compromised. *See* 38 U.S.C. § 5724(a)(1).

Because the plaintiffs were awarded appropriate relief and because the VA conducted an adequate IRA of the data breach, the court finds that the VA did not fail to take agency action it was required to take with respect to count eight.

Conclusion

Having considered the foregoing and being of the opinion that the plaintiffs have failed to properly state any claims challenging final agency action under the Administrative Procedures Act, 5 U.S.C. § 551 *et seq*., the court finds that Counts Two, Five, Six, and Eight shall be **DISMISSED**. The court shall so rule by separate order.

DONE and **ORDERED**, this the 21st day of April 2010.

INGE PRYTZ JOHNSON
U.S. DISTRICT JUDGE