epic.org | ELECTRONIC PRIVACY INFORMATION CENTER

COMMENTS OF THE ELECTRONIC PRIVACY INFORMATION CENTER

to the

FEDERAL TRADE COMMISSION

Safeguards Rule, 16 CFR 314, Project No. P145407

Standards for Safeguarding Customer Information Request for Public Comment

[Docket No. 2016-21231]

November 7, 2016

By notice published on September 7, 2016, the Federal Trade Commission ("FTC") requests public comments on its Standards for Safeguarding Customer Information ("Safeguards Rule").[1] Pursuant to this notice, the Electronic Privacy Information Center ("EPIC") submits these comments to urge the FTC to (1) expand the scope of the Safeguards Rule to include all organizations and companies that collect consumer data; (2) clarify that compliance with the Safeguards Rule Guidance is mandatory; and (3) establish a data minimization requirement for organizations that are subject to the Safeguards Rule.

EPIC is a public interest research center in Washington, D.C. EPIC was established in 1994 to focus public attention on emerging privacy and related human rights issues, and to

[1] *Standards for Safeguarding Customer Information*, 81 Fed. Reg. 61,632 (Sep. 7, 2016) [hereinafter "Safeguards Rule Request for Comments].

protect privacy, the First Amendment, and constitutional values. EPIC has long advocated for strong privacy and security safeguards for consumer information held by financial, educational, and commercial organizations.[2] EPIC has played a leading role in developing the authority of the FTC to address emerging privacy issues and to safeguard the privacy rights of consumers.[3] EPIC also filed an amicus brief in *FTC v. Wyndham*, defending the FTC's "critical role in safeguarding consumer privacy and promoting stronger security standards."[4] EPIC has previously testified before Congress on the need for financial institutions and companies to protect consumers against data breaches.[5]

---

[2] *See e.g.*, *Comments of the Electronic Privacy Information Center to the Federal Trade Commission "Public Workshop and Request for Public Comments and Participation"* May 27, 2011, https://epic.org/privacy/idtheft/EPIC_Debt_Collection_Comments.pdf ("EPIC Debt Collection Comments)"; *Comment of the Electronic Privacy Information Center to The Office of Science and Technology Policy Request for Information: Big Data and the Future of Privacy,* Apr. 4, 2014, https://epic.org/privacy/big-data/EPIC-OSTP-Big-Data.pdf; *EPIC Comments In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services,* Jul. 6, 2016, https://www.epic.org/apa/comments/EPIC-FCC-Privacy-NPRM-2016.pdf.

[3] *See, e.g.,* Letter from EPIC Exec. Dir. Marc Rotenberg to FTC Comm'r Christine Varney (Dec. 14, 1995) (urging the FTC to investigate the misuse of personal information by the direct marketing industry), http://epic.org/privacy/internet/ftc/ftc_letter.html; DoubleClick, Inc., FTC File No. 071-0170 (2000) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/internet/ftc/DCLK_complaint.pdf; Microsoft Corporation, FTC File No. 012 3240 (2002) (Complaint and Request for Injunction, Request for Investigation and for Other Relief), http://epic.org/privacy/consumer/MS_complaint.pdf; Choicepoint, Inc., FTC File No. 052-3069 (2004) (Request for Investigation and for Other Relief) , http://epic.org/privacy/choicepoint/fcraltr12.16.04.html; In the Matter of Snapchat, Inc. (2013) (Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/ftc/EPIC-Snapchat-Complaint.pdf; In the Matter of Scholarships.com, LLC (2013) (Complaint, Request for Investigation, Injunction, and Other Relief), https://epic.org/privacy/student/EPIC-FTC-Compl-Scholarships.com.pdf.

[4] Brief of Amicus Curiae Electronic Privacy Information Center et al., in Support of Respondent, *FTC v. Wyndham Hotels & Resorts, LLC*, 799 F.3d 236 (3d Cir. 2015), https://epic.org/amicus/ftc/wyndham/Wyndham-Amicus-EPIC.pdf.

[5] *See, e.g.*, Testimony and Statement for the Record of Marc Rotenberg, Executive Director, Electronic Privacy Information Center on "Cybersecurity and Data Protection in the Financial Sector," Before the Senate Committee on Banking, Housing, and Urban Affairs, June 21, 2011, https://epic.org/privacy/testimony/EPIC_Senate_Banking_Testimony%20_6_21_11.pdf; Testimony and Statement for the Record of Marc Rotenberg, Executive Director, Electronic Privacy Information Center, Hearing on the Discussion Draft of H.R. ____, A Bill to Require Greater Protection for Sensitive Consumer Data and Timely Notification in Case of Breach, Before the House Committee on Energy and Commerce Subcommittee on Commerce, Manufacturing, and Trade, June 15, 2011, http://epic.org/privacy/testimony/EPIC_Testimony_House_Commerce_6-11_Final.pdf.

I. AMERICANS FACE A DATA BREACH EPIDEMIC

The unregulated collection of personal data has led to staggering increases in identity theft, security breaches, and financial fraud in the United States.[6] The recent Yahoo! data breach that exposed the personal information of at least half-a-billion users[7] is the latest in a growing number of high-profile hacks that threaten the privacy, security, and financial stability of American consumers. Far too many organizations collect, use, and disclose detailed personal information with too little regard for the consequences.

Not surprisingly, the privacy concerns of Americans are increasing at a rapid rate. Industry expert Mary Meeker's most recent Internet Trend report said simply, "[a]s data explodes . . . data security trends explode."[8] According to Meeker, 45 percent of users "are more worried about their online privacy than one year ago" and 74 percent have limited their online activity in the last year due to privacy concerns."[9] Public opinion polls show that 91 percent of Americans believe they have lost control of how companies collect and use their personal information.[10] And a recent government study found that nearly half of American internet users refrain from online activities due to privacy and security concerns.[11] According to the Pew

---

[6] *See, e.g.*, Fed. Trade Comm'n, *Consumer Sentinel Network Data Book* (Feb. 2016), https://www.ftc.gov/system/files/documents/reports/consumer-sentinel-network-data-book-january-december- 2015/160229csn-2015databook.pdf.
[7] Yahoo!, *An Important Message to Yahoo Users on Security* (Sept. 22, 2016), https://investor.yahoo.net/releasedetail.cfm?ReleaseID=990570.
[8] Mary Meeker, *Internet Trends 2016 – Code Conference*, KPCB (June 1, 2016), http://www.kpcb.com/internettrends.
[9] *Id*.
[10] Lee Rainie, *The State of Privacy in Post-Snowden America*, PEW RESEARCH CENTER (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america.
[11] Rafi Goldberg, Lack of Trust in Internet Privacy and Security May Deter Economic and Other Online Activities, NAT'L TELECOMM. AND INFO. ADMIN. (May 13, 2016), https://www.ntia.doc.gov/blog/2016/lack-trust-internetprivacy-and-security-may-deter-economic-and-other-online-activities.

Research Center, "A majority of the U.S. public believes changes in law could make a difference in protecting privacy – especially when it comes to policies on retention of their data."[12]

The Yahoo! breach is one of more than 800 data breaches that have occurred in 2016 alone, which have exposed nearly 30 million records at healthcare providers, educational institutions, businesses, financial institutions, and various levels of government since the beginning of this year.[13]

In 2016 alone, the financial sector has so far experienced 36 data breaches that have exposed more than 26,262 records.[14] According to a financial services breach report by security firm Bitglass, five of the nation's largest banks have already suffered a breach in the first half of 2016 alone.[15] The report also found that data breaches for the banking industry nearly doubled from 2014 to 2015.[16] Credit bureau Experian experienced a data breach in 2015 that exposed approximately 15 million Social Security numbers and other personal information. A 2014 cyberattack on JPMorgan Chase, the largest bank in the nation, compromised the accounts of an estimated 76 million households and 7 million small businesses.[17]

EPIC had previously testified before Congressional committees in the U.S. Senate and House of Representatives concerning cybersecurity and data protection in the financial sector.[18]

---

[12] Lee Rainie, *The State of Privacy in Post-Snowden America*, PEW RESEARCH CENTER (Sept. 21, 2016), http://www.pewresearch.org/fact-tank/2016/01/20/the-state-of-privacy-in-america.
[13] *Identity Theft Resource Center: 2016 Data Breach Category Summary*, http://www.idtheftcenter.org/images/breach/ITRCBreachStatsReportSummary_2016.pdf (last updated Nov. 1, 2016).
[14] *Id* at 4.
[15] *Bitglass Report: Lost and Stolen Devices Account for One in Four Breaches in the Financial Services Sector*, BITGLASS (Aug. 25, 2016). http://www.bitglass.com/press-releases/financial-services-breach-report-2016.
[16] *Id*.
[17] Jessica Silver-Greenberg, Matthew Goldstein, & Nicole Perlroth, *JPMorgan Chase Hacking Affects 76 Million Households*, N.Y. TIMES (Oct. 2, 2014), http://dealbook.nytimes.com/2014/10/02/jpmorgan-discovers-further-cyber-security-issues/.
[18] *See* Testimony and Statement for the Record of Marc Rotenberg, Executive Director, Electronic Privacy Information Center on "Cybersecurity and Data Protection in the Financial Sector," Before the

EPIC warned of the significant costs to consumers following financial sector data breaches, and argued that current laws to not adequately protect consumers. EPIC also recommended legislation that strengthens safeguards for consumer information and promotes data minimization practices. "These techniques reduce the risk of cyber attack and minimize the risk to consumers when attacks occur," EPIC said.[19]

Educational institutions engaging in financial activities have also experienced serious data breach incidents. The education sector has experienced 74 data breaches in 2016 so far, which has exposed nearly half-a-million records.[20] In 2014, EPIC filed a complaint with the FTC against Maricopa County Community College District ("MCCCD") after the data of almost 2.5 million former students, employees, and vendors was compromised.[21] The compromised data included names, mailing and e-mail addresses, Social Security Numbers, dates of birth, demographic information, academic, and financial information. EPIC urged the FTC to investigate MCCCD for repeated violations of the Safeguards Rule for disclosure of non-public personal information to third-parties, failure to conduct testing and monitoring of its security systems, and failure to improve security programs following a breach in 2011. The FTC failed bring an enforcement action against MCCCD over its violations of the Safeguards Rule.

MCCCD is hardly the only institution of higher education that has been subject to a data breach in recent years. In 2014, a database at the University of Maryland was breached that

---

Senate Committee on Banking, Housing, and Urban Affairs (June 21, 2011) https://epic.org/privacy/testimony/EPIC_Senate_Banking_Testimony%20_6_21_11.pdf; Testimony and Statement for the Record of Marc Rotenberg, Executive Director, Electronic Privacy Information Center on "Cybersecurity and Data Protection in the Financial Sector," Before the House Committee on Financial Services (Sept. 14, 2011), https://epic.org/privacy/testimony/EPIC_Testimony_HCFS_9-11-1.pdf.

[19] *Id*. at 12.

[20] *Identity Theft Resource Center: 2016 Data Breach List*, http://www.idtheftcenter.org/images/breach/ITRCBreachReport_2016.pdf (last updated Nov. 1, 2016).

[21] In the Matter of Maricopa County Community College District (2014) (EPIC Complaint, Request for Investigation, Injunction, and Other Relief) https://epic.org/privacy/student/EPIC-Safeguards-Rule-Complaint.pdf.

contained the data of more than 300,000 students, faculty, and staff over 20 years.[22] In 2014, Johns Hopkins experienced a data breach that compromised the names and contact information of more than 800 students who attended the school over a seven-year period. That same year, Indiana University reported it had stored names, addresses, and Social Security numbers of more than 100,00 students and recent graduates in an insecure location, exposing them to identity theft and other forms of fraud.[23]

In light of the rising frequency and severity of data breaches, the FTC must respond with comprehensive, legally enforceable data security rules that apply broadly to all entities that handle consumer information.

II. THE FTC MUST IMPLEMENT AND ENFORCE COMPREHENSIVE DATA SECURITY STANDARDS

The FTC's authority under the Gramm-Leach-Bliley Safeguards Rule is an essential tool for protecting consumer information. Given the growing risk to American consumers of data breach, identity theft, and financial fraud, the FTC must enforce the Safeguards Rule. EPIC supports the FTC's guidance on complying with the Safeguards Rule ("Safeguards Rule Guidance"), which specifies basic security measures for protecting data.[24] However, the FTC must clarify that compliance with its guidance on the Safeguards Rule is mandatory and enforceable through fines and penalties. In addition, personal information is increasingly held across a variety of industries and EPIC urges the FTC to modify its application of the Safeguards Rule to reflect this trend. Finally, EPIC recommends strengthening the Safeguards Rule by

[22] Letter from President Loh, Letter from Brian D. Voss concerning UMD Data Breach, http://www.umd.edu/datasecurity/.
[23] Johns Hopkins Statement: Breach of a University Server, Mar. 7, 2014, http://releases.jhu.edu/2014/03/07/server-breach/; Indiana University Reports Potential Data Exposure, Feb. 25, 2014, http://news.iu.edu/releases/iu/2014/02/data-exposure- disclosure.shtml.
[24] *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, FED. TRADE COMM'N (Apr. 2006), https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying [hereinafter "Safeguards Rule Guidance"].

including data minimization requirements that require companies to collect only information needed to fulfill a specified purpose and to retain it only as long as needed to fulfill that purpose.

A. The FTC Must Mandate and Enforce Compliance with the Safeguards Rule Guidance

As described in Section I, financial institutions within the existing scope of the Safeguards Rule continue to experience data breaches due to inadequate security measures. To date, the agency has maintained that the legal standard mandating "appropriate" security measures will be enforced according to each company's "size and complexity, the nature and scope of its activities, and the sensitivity of the customer information it handles."[25] There are, however, rudimentary measures that every financial institution should take regardless of individual circumstances. Data breaches expose Social Security numbers, credit card information, names, addresses, telephone numbers, and other types of private, personally identifiable information to criminals. This exposes consumers to a range of harms, most significantly identity theft. The agency should clarify that the standard security practices published in its April 2006 guidelines implementing the Gramm-Leach-Bliley Safeguards Rule, titled "Financial Institutions and Customer Information: Complying with the Safeguards Rule,"[26] are legally binding and therefore mandatory.

EPIC has previously recommended that the following practices from the FTC's Safeguards Rule Guidance be mandatory:

- Checking references or doing background checks before hiring employees who will have access to customer information;
- Limiting access to customer information to employees who have a business reason to see it;
- Locking rooms and file cabinets where records are kept;

[25] Safeguards Rule Guidance.
[26] *Id*.

- Referring calls or other requests for customer information to designated individuals who have been trained in how your company safeguards personal data;
- Reporting suspicious attempts to obtain customer information to designated personnel;
- Avoiding the storage of sensitive customer data on a computer with an Internet connection;
- Ensuring that customer information is only stored on a computer with a "strong" password, kept in a physical-secure area;
- Maintaining a careful inventory of the company's computers and any other equipment on which customer information may be stored;
- Encrypting any sensitive data transmitted over the Internet, for instance by e-mail;
- Disposing of customer information in a secure way and in compliance with the FTC's Disposal Rule;
- Designating or hiring a records retention manager to supervise the disposal of records containing customer information;
- Maintaining up-to-date and appropriate programs and controls to prevent unauthorized access to customer information; and
- Keeping logs of activity on internal networks with access to sensitive data and monitoring them for signs of unauthorized access to customer information.[27]

If a company fails to comply with its obligation to safeguard personal data that it chooses to possess, it must be held accountable.

B. The Safeguards Rule Must Be Expanded to All Entities that Handle Consumer Information

The FTC poses the following question:

> Should the Safeguards Rule's definition of ''financial institution'' be modified to also include entities that are significantly engaged in activities that the Federal Reserve Board has found to be incidental to financial activities? Should it also include activities that have been found to be closely related to banking or incidental to financial activities by regulation or order in effect after the enactment of the G-L-B Act?[28]

[27] *Id*. at 3; *Comments of the Electronic Privacy Information Center to the Federal Trade Commission "Public Workshop and Request for Public Comments and Participation"* May 27, 2011, https://epic.org/privacy/idtheft/EPIC_Debt_Collection_Comments.pdf.
[28] Safeguards Rule Request for Comments at 61,635.

Yes, and yes. EPIC urges the FTC to include organizations that perform "incidental" financial activities and activities found to be "closely related to banking or incidental to financial activities" after passage of the G-L-B Act.[29] These "incidental" activities should include, but not be limited to, educational institutions and commercial businesses that process information about students or consumers. These organizations frequently collect the same sensitive information collected by traditional financial institution, and are subject to the same security threats. Thus, these entities should be required to abide by the same security requirements to safeguard consumer data.

EPIC also urges the FTC to apply the Rule to all "consumer" information maintained by financial institutions, rather than limiting protections only to information of "customers" that have a continuing relationship with the entity.[30] Companies such as data brokers and advertising networks collect massive amounts of sensitive information on American consumers without ever establishing a "customer relationship" with those consumers. Consumers should not be left defenseless simply because these companies collect their information without their knowledge or consent.

C. The Safeguards Rule Should Be Modified to Require Data Minimization

The FTC also asks, "What modifications, if any, should be made to the Rule to increase its benefits to consumers?"[31]

EPIC recommends that the FTC strengthen the Safeguards Rule by adding enforceable data minimization requirements. EPIC has long argued that the best way to prevent loss or

[29] *Id*.
[30] 16 CFR 313.3(h), (i). The Safeguards Rule uses the definitions of ''customer'' and ''customer relationship'' from the Privacy Rule. 16 CFR 314.2(a).
[31] Safeguards Rule Request for Comments at 61,634.

misuse of sensitive personal information is to avoid gathering or storing it in the first place.[32] Data that is not collected or retained cannot be subject to unauthorized access or disclosure. Minimizing stored user data reduces incentives for hackers to attack data storage systems by reducing the amount of data available to steal. This practice also reduces the costs of data breaches. Data minimization is actually more effective at protecting the confidentiality of consumer data than notice and choice: "most harms are not mitigated through notice or control alone, but require security and data minimization."[33]

Strong privacy protections are also a necessary and pragmatic part of risk mitigation in the age of the ubiquitous cybersecurity breach. Failure to protect user privacy frequently stems from failure to adequately secure user data, which can result in enormous liability for companies.[34] The more data a company stores, the more valuable a target its database is for hackers; and the more stored data, the greater the company's losses in the event of a breach.[35] Adding data minimization requirements to the Safeguards Rule would significantly strengthen the Rule and benefit consumers.

---

[32] *See, e.g.*, Reply Comments of EPIC, *In the Matter of Protecting the Privacy of Customers of Broadband and Other Telecommunications Services* 11-12, WC Docket NO. 16-106 (July 6, 2016), https://epic.org/apa/comments/EPIC-FCC-Privacy-NPRM-Reply-Comments-07.06.16.pdf; Comments of EPIC, Request for Information: Big Data and the Future of Privacy (April 4, 2014), https://epic.org/privacy/big-data/EPIC-OSTP-Big-Data.pdf; Brief of Amicus Curiae Electronic Privacy Information Center in Support of Respondent, *City of Ontario v. Quon*, 560 U.S. 746 (2010), https://epic.org/privacy/quon/Quon_Brief_Draft_final.pdf.

[33] Rebecca Balebako, Cristian Bravo-Lillo, & Lorrie Faith Cranor, *Is Notice Enough: Mitigating the Risks of Smartphone Data Sharing*, 11 J. L. & POL'Y FOR INFO. SOC'Y 279, 314 (2015).

[34] *2016 Cost of Data Breach Study: United States*, PONEMON INST., 1 (June 2016).

[35] Bruce Schneier, *Data Is A Toxic Asset*, SCHNEIER ON SECURITY, (March 4, 2016), https://www.schneier.com/blog/archives/2016/03/data_is_a_toxic.html ("saving [data] is dangerous because failing to secure it is damaging. It will reduce a company's profits, reduce its market share, hurt its stock price, cause it public embarrassment, and—in some cases—result in expensive lawsuits and occasionally, criminal charges. All this makes data a toxic asset, and it continues to be toxic as long as it sits in a company's computers and networks.").

III. CONCLUSION

For the foregoing reasons, EPIC urges the FTC to (1) expand the scope of the Safeguards Rule to include all organizations and companies that collect consumer data; (2) emphasize that the FTC's Safeguards Rule Guidance is mandatory; and (3) establish a data minimization requirement for organizations that are subject to the Safeguards Rule.

Given the increased scope of identity theft and data breaches across a wide array of industries and organizations, the FTC should adopt these measures. This will only benefit consumers and organizations alike by minimizing the myriad costs that result from data insecurity.

Respectfully Submitted,

/s/ Marc Rotenberg
Marc Rotenberg
EPIC President and Executive Director

/s/ Claire Gartland
Claire Gartland
Director, EPIC Consumer Privacy Project

/s/ Kimberly Miller
Kimberly Miller
EPIC Administrative Law Fellow