Testimony of Edmund Mierzwinski,

U.S. PIRG Consumer Program Director

Hearing on "Data Security: Vulnerabilities and Opportunities for Improvement"

Before the House Committee on Financial Services,

Subcommittee on

Financial Institutions and Consumer Credit

Honorable Blaine Luetkemeyer, Chair

1 November 2017

Testimony of Edmund Mierzwinski, U.S. PIRG Consumer Program Director Before the Committee on Financial Services, Subcommittee on Financial Institutions and Consumer Credit

Chairman Luetkemeyer, Representative Lacy Clay, members of the committee, I appreciate the opportunity to testify before you on the important matter of data security and cyber threats. Since 1989, I have worked on data privacy issues, among other financial system and consumer protection issues, for the U.S. Public Interest Research Group. The state PIRGs are non-profit, non-partisan public interest advocacy organizations that take on powerful interests on behalf of their members.

Summary:

As stated in the committee's staff memo: "Congress must thoroughly examine data security vulnerabilities and the shortcomings of the existing federal and state regulatory regimes to identify any gaps in data security regulation and highlight opportunities for reform."

I construe data security and the issues it raises broadly in this testimony to include an examination not only of data security and proper data breach response. I also review the history of how public policy decisions trending against the concept of consumer privacy have encouraged and promoted greater collection, sale and sharing of consumer information – without concomitant consumer control, without adequate regulatory requirements for data security, and certainly without market incentives for firms to protect the consumer financial DNA they collect and then sell.

I urge the Congress, at a minimum, to enact free credit freeze legislation. I caution the Congress, however, not to move forward on any breach or data security legislation that would preempt strong state privacy leadership or would endorse closed or non-technology neutral standards. Federal law should never become a ceiling of protection, it should always serve as a minimal floor that allows state experimentation. Further, federal law should not endorse specific solutions that limit innovation.

I. Introduction:

While I note that thorough questioning by members at the previous committee hearing featuring Richard Smith, the ***ex-CEO*** of Equifax, helped to confirm numerous problems with Equifax security and its response to the breach, it is telling that Equifax and its competitor Big 3 consumer credit reporting agencies Experian and Transunion all chose to ignore Congressional requests to send their current CEOs to that continuation hearing. What do they have to hide?

The authoritative Privacy Rights Clearinghouse has estimated that at least 1,073,490,127 records have been breached in a total of at least 7,730 data breach occurrences made public since 2005.[1] The latest exploit, against Equifax, a major consumer credit reporting agency (colloquially, a credit bureau), not only affected at least 145.5 million consumers, but compromised perhaps the richest trove of personal information I have seen in my over

[1] See Data Breach page at Privacy Rights Clearinghouse, last visited 30 October 2017, https://www.privacyrights.org/.

years of privacy and data security research.[2] While Yahoo[3] now says all 3 billion of its user accounts may have been breached in 2013, much of the information taken could only be used for "phishing" emails or "social engineering" phone calls designed to use a little information to try to gain a lot more. While the Target[4] and other retail breaches resulted in the theft of millions of credit and debit card numbers, those numbers can only be used in the short-term for "existing account fraud" before banks change the numbers.

A. The Loss By Equifax Of The Bits And Pieces Of Your Financial DNA Is Worse Than A Card Breach:

Dates of birth and Social Security Numbers do not change. They do not have a shelf life and can be used for more serious identity theft such as hard-to-deal-with new account fraud, tax refund fraud, and theft of medical services. To me, the Equifax breach is rivaled only by the loss of similar information for 22 million employees, applicants and even friends providing character references for those applicants by the U.S. Office of Personnel Management (OPM)[5] in 2015.

Unlike credit card numbers, your Social Security Number and Date of Birth don't change and may even grow more valuable over time, like gold in a bank vault. Much worse, they are the keys to "new account identity theft," which can only be prevented by a credit report freeze, as discussed in detail at the last hearing.[6] While Equifax and other consumer credit reporting companies are required by the Fair Credit Reporting Act (FCRA) to make it hard for imposters to obtain another's credit report (how many security questions did you answer to obtain your own report?); identity thieves don't want your credit report. Instead, they use your SSN and DOB to apply for credit in your name; so that the bank or other creditor, which is a trusted third party (and likely answers no security questions) with easy access to the credit reporting company, obtains your credit report and/or credit score and then wrongly issues credit to the thief. In the U.S., such new account identity theft is fueled both by the high demand for "instant credit" and by that critical flaw in our credit granting system, where SSNs serve as both a matching identifier in databases and as an authenticator of a consumer applicant.[7]

---

[2] Equifax's primary and best-known business is as one of three (Experian and Transunion are the others) national "Consumer Reporting Agencies" (colloquially "credit bureaus") that do their consumer reporting business under the Fair Credit Reporting Act (FCRA) but also engage in a wide variety of lightly to unregulated direct marketing as "data brokers."

[3] Lily Hay-Newman, "Yahoo's 2013 Email Hack Actually Compromised Three Billion Accounts," 3 October 2003, https://www.wired.com/story/yahoo-breach-three-billion-accounts/

[4] The Target breach reportedly exposed 40 million credit and debit card numbers, as well as the customer account records – including phone numbers and emails -- of millions more consumers. See Eric Dezenhall, "A Look Back at the Target Breach," 6 June 2015, https://www.huffingtonpost.com/eric-dezenhall/a-look-back-at-the-target_b_7000816.html

[5] Brendan I. Koerner, "Inside the Cyberattack That Shocked the US Government," 23 October 2017, https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/

[6] See testimony of Mike Litt, U.S. PIRG before the committee, 25 October 2017, available at https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-mlitt-20171025.pdf

[7] See "Security In Numbers: SSNs and Identity theft," an FTC report, which discusses the problems of using Social Security Numbers to authenticate people even though they are not secret, but ubiquitous and widely available to thieves, December 2008, available at https://www.ftc.gov/sites/default/files/documents/reports/security-numbers-social-security-numbers-and-identity-theft-federal-trade-commission-report/p075414ssnreport.pdf

B. And Even Worse, The Equifax Breach Was By A Data Broker: A Firm With Only One Job—Buying And Selling Consumer Information:

Equifax should do better at protecting data: it is a data broker, not a corner store, department store, health care provider or government agency. Incredibly, this is not the first security problem Equifax has faced recently.[8]

Equifax should have had a deeper moat and thicker castle walls, with more cross-bow archers, more trebuchets and more cauldrons of boiling oil on the watchtowers to defend your data than a merchant or even a government agency. It did not.

Regarding the committee's specific Equifax hearings, I associate my remarks completely with all recommendations of my consumer advocacy colleagues and state attorneys general experts at the committee's "Continuation of the Equifax Hearing" requested by Ranking Member Maxine Waters (CA), last week.[9] Of course, I also believe that the minimum action Congress should take would be to extend free credit freezes at all 3 national consumer reporting agencies to all consumers at all times. The committee should also ensure one-stop shopping for credit freezes, as is already the law for fraud alerts. You should need to contact only one credit bureau to gain protection at all three.

C. The Paradox of Equifax: Highly Regulated When It Sells Credit Reports Yet Not Really Regulated When It Sells Other Products as a Data Broker

The Paradox of Consumer Credit Reports vs. Other Data Products: The Equifax breach extensively reviewed in two previous full committee hearings demonstrates several paradoxes of our data use, privacy and data security laws and regulations. While the security of the ***consumer credit reports*** sold by Equifax in its role as a Consumer Reporting Agency (CRA) is strictly regulated by the Fair Credit Reporting Act (FCRA);[10] the security of the ***Social Security Numbers and Dates of Birth and other personally-identifiable-information (PII)*** lost in the breach is regulated only under the limited data security requirements of Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.).[11] In addition, other (non-credit report) consumer profiles sold by Equifax and its hundreds, or thousands, of competitors in the ***data broker*** business are hardly regulated at all.

---

[8] Thomas Fox-Brewster, "A Brief History of Equifax Security Fails," 8 September 2017, Forbes. https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#192afb0a677c

[9] Continuation of Hearing entitled "Examining the Equifax Data Breach," 25 October 2017, witness statements available at https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=402472

[10] 15 U.S.C. 1681 *et seq.*

[11] The prudential regulator rules implementing Title V of GLBA generally only require that a breach notice plan be "considered." See bank regulators' joint "Interagency Guidelines Establishing Information Security Standards" are available at: https://www.fdic.gov/regulations/laws/rules/2000-8660.html The FTC Safeguards Rule applicable to national consumer credit reporting agencies including Equifax, which is silent on breach notification, is available here: https://www.ftc.gov/sites/default/files/documents/federal_register_notices/standards-safeguarding-customer-information-16-cfr-part-314/020523standardsforsafeguardingcustomerinformation.pdf The FTC is currently adding elements of a breach notification plan to its 2002 final rule above. All documents related to Title V are archived by the FTC here: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule

The Federal Trade Commission has recognized this. In two major reports in the last 5 years, it has called for greater authority to regulate the collection, sharing and sale of consumer information outside the limited walls of the FCRA, which primarily applies only to reports used in the determination of a consumer's eligibility for credit, insurance or employment. From the FTC's landmark report recommending Congress give it more authority over data brokers:[12]

> "Data brokers obtain and share vast amounts of consumer information, typically behind the scenes, without consumer knowledge. Data brokers sell this information for marketing campaigns and fraud prevention, among other purposes. Although consumers benefit from data broker practices which, for example, help enable consumers to find and enjoy the products and services they prefer, data broker practices also raise privacy concerns. […] Data brokers combine and analyze data about consumers to make inferences about them, including potentially sensitive inferences such as those related to ethnicity, income, religion, political leanings, age, and health conditions. Potentially sensitive categories from the study are "Urban Scramble" and "Mobile Mixers," both of which include a high concentration of Latinos and African-Americans with low incomes. The category "Rural Everlasting" includes single men and women over age 66 with "low educational attainment and low net worths." Other potentially sensitive categories include health-related topics or conditions, such as pregnancy, diabetes, and high cholesterol."

When the Big 3 credit bureaus are in their alternate guise as nearly unregulated data brokers, they sell numerous consumer profiles to businesses. Consumers have no rights to know about these files, to examine these files, to correct these files or to limit their use. Congress should consider the FTC's proposals.

- The data broker Experian:[13] "New markets targeted. Response rates improved. Revenue increased. These are the results we at Experian, as the industry leader, help you achieve with our business services."
- The data broker Equifax:[14] "The power behind our solutions—and your acquisition programs—is the superior quality of our data."
- The data broker Transunion:[15] "TransUnion offers more complete and multidimensional information for informed decisions that create opportunities for your business."

Paradox: the FCRA is One of our Strongest Privacy Laws: Despite the abysmal failure over the years of firms regulated under the FCRA to maintain the accuracy of consumer credit reports, or to adequately respond to consumers who dispute the inaccuracies that harm their financial or employment opportunities,[16] it remains that the 1970 FCRA's framework is fundamentally based on the Code of Fair Information Practices (FIPs), developed by a committee of the HEW Advisory Committee on Automated Data Systems in 1972, which was codified in the

[12] FTC News Release, "Agency Report Shows Data Brokers Collect and Store Billions of Data Elements Covering Nearly Every U.S. Consumer," 27 May 2014, https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more

[13] http://www.experian.com/business-services/business-services.html

[14] http://www.equifax.com/business/acquire-more-customers

[15] https://www.transunion.com/business

[16] "…the credit reporting agencies have grown up in a culture of impunity, arrogance, and exploitation. For decades, they have abused consumers, cut corners in personnel and systems, and failed to invest in measures that would promote accuracy or handle disputes properly." See page 3, testimony of Chi Chi Wu, National Consumer Law Center, before the committee on 25 October 2017, available at https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-ccwu-20171025.pdf

1974 U.S. Privacy Act and governs information use by federal agencies.[17] The Privacy Rights Clearinghouse notes:

> "In contrast to other industrialized countries throughout the world, the U.S. has not codified the Fair Information Principles into an omnibus privacy law at the federal level. Instead, the Principles have formed the basis of many individual laws in the U.S., at the both federal and state levels -- called the "sectoral approach." Examples are the Fair Credit Reporting Act, the Right to Financial Privacy Act, the Electronic Communications Privacy Act, and the Video Privacy Protection Act.[18]"

The FIPs are nevertheless embodied in the FCRA: The FCRA limits the use of consumer credit reports only to firms with certain permissible purposes (generally, determinations of a consumer's eligibility for credit, insurance and employment), it requires credit bureaus (data collectors) to meet certain accuracy standards and it allows consumers to review their files, dispute and demand corrections of mistakes and to control the secondary use of their files by opting out of marketing uses of their reports.

Nevertheless, the U.S. sectoral-only privacy laws should be contrasted with the new European **General Data Protection Regulation (GDPR).** It provides over-arching privacy rights to European citizens over corporate usage of their information, including rights to control the use of their information and to seek redress (and compensation) against the infringing company. Importantly, the GDPR, when it goes into final effect next year, trumps the existing Privacy Shield[19] applicable to U.S. firms doing business in Europe and provides a roadmap for U.S. companies to improve their treatment of U.S. consumers.[20]

In particular, since SIFMA member firms will be subject to the GDPR, it seems that they can import those protections to small investors in the U.S., rather than seek, as they may today, to weaken applicability of existing state data security and identity theft laws.

The Paradox of Identity Theft as a Business Opportunity: The big credit bureaus have responded to the scourge of identity theft driven by instant credit, sloppy credit report-granting practices, and of course, data breaches, not by improving their own security and compliance but by seizing new business opportunities:

Consumers scared of either fraud and identity theft or low credit scores are urged to buy their subscription credit monitoring services, for as much as $10-20/month. The GAO has determined that such "services offer some benefits but are limited in preventing fraud."[21] Estimates are that consumers spend at least $3 billion/year on credit monitoring services.[22]

---

[17] "U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens viii (1973)", https://epic.org/privacy/consumer/code_fair_info.html

[18] Privacy Rights Clearinghouse, "A Review of The Fair Information Principles: The Foundation Of Privacy Public Policy," 1 October 1997, https://www.privacyrights.org/blog/review-fair-information-principles-foundation-privacy-public-policy

[19] For information on the Privacy Shield, see https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield

[20] The GDPR is explained here https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

[21] U.S. General Accounting Office, March 2017: "Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud," http://www.gao.gov/assets/690/683842.pdf

[22] Steve Weisman, "Is Identity Theft Protection Worth It?", 22 April 2017, USA Today, https://www.usatoday.com/story/money/columnist/2017/04/22/identity-theft-protection-worth/100554362/

Despite that the bureaus have failed to either protect credit reports or maintain the "maximum possible accuracy" required by law, they have also monetized a lucrative business-to-consumer (B2C) channel for over 20 years to market their over-priced, under-performing credit monitoring products.[23]

And of course, the big credit bureaus and others have also leapt into the business of B2B identity validation and verification, largely in response to their own, and others', failure to maintain the security of information.

The Paradox of Businesses as Customers and Consumers as Products: Despite nearly 50 years of FCRA requirements to handle consumer disputes and over 20 years of aggressive-direct-to-consumer advertising of pricy subscription-based credit monitoring products, its ex-CEO repeatedly apologized to Congress that, as a business-to-business company, it had no idea how many consumers would call or email. How is this possible? Well, it turns out consumers are not looked at by Equifax as customers.

This absurd disconnect is because of a market failure in credit reporting; we are not their customers, we are their product. The consumer credit reporting market is dominated by the Big 3 gatekeepers to financial and employment opportunity. Yet, you cannot choose a credit bureau. When you are mad at your bank's fees or policies, you can vote with your feet and find a new bank. You're stuck with the credit bureaus. Richard Cordray, director of the Consumer Financial Protection Bureau, often calls credit reporting one of several "dead-end markets" in need of stricter regulation to counter that market failure.[24]

The Big 3 bureaus (Equifax, Experian and Transunion) were fined an inadequate total of $2.5 million by the Federal Trade Commission (in 2000) for failing to have enough employees to answer the phones to handle their complaints.[25]

Nevertheless, we are encouraged by the recent efforts by the Consumer Bureau to achieve changes to the Big 3's operations through supervision.[26]

Consumers Have Little Control of their Information: The 1999 Gramm-Leach-Bliley Financial Modernization Act was largely enacted to allow mergers of commercial banks, investment banks, securities firms and insurance companies. However, due to privacy complaints at the time about a number of large banks, including U.S. Bank,

---

[23] On 7 September 2017, the date that the Equifax breach was announced to the public, the committee held a hearing on a discussion draft from Mr. Royce, a bill which we oppose. The bill would exempt credit bureau marketing and education programs from the Credit Repair Organizations Act, and exempt the bureaus, and others that might seek the same license, from strong consumer protection laws. The discussion draft is available at https://financialservices.house.gov/uploadedfiles/bills-115_royce020_pih.pdf We concur with Chi Chi Wu's testimony against both the Royce bill and against a bill from Mr. Loudermilk also discussed that day. HR2359, the so-called FCRA Liability Harmonization Act, would eliminate punitive damages and cap other damages in actions brought under the FCRA. Testimony of Chi Chi Wu, National Consumer Law Center is available at https://financialservices.house.gov/uploadedfiles/hhrg-115-ba15-wstate-ccwu-20170907.pdf

[24] Richard Cordray, "Prepared Remarks of CFPB Director Richard Cordray at the National Association of Attorneys General," 23 February 2015, https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-of-cfpb-director-richard-cordray-at-the-national-association-of-attorneys-general-2/

[25] Press release, "Nation's Big Three Consumer Reporting Agencies Agree To Pay $2.5 Million To Settle FTC Charges of Violating Fair Credit Reporting Act," 13 January 2000, available at https://www.ftc.gov/news-events/press-releases/2000/01/nations-big-three-consumer-reporting-agencies-agree-pay-25

[26] Consumer Financial Protection Bureau, "Supervisory Highlights: Consumer Reporting, Special Edition," March 2017, Issue 14, Winter 2017, available at http://files.consumerfinance.gov/f/documents/201703_cfpb_Supervisory-Highlights-Consumer-Reporting-Special-Edition.pdf

which was sued by the State of Minnesota for sharing customer records with a third-party telemarketer that then preyed on its customers,[27] the law did include a modest privacy and data security provision, Title V, that gave consumers the ability to opt-out of sharing of their personal information only with non-affiliated, non-financial firms (but explicitly allowed sharing with affiliates or other financial firms, regardless of a consumer's wishes).[28] A wide variety of organizations, ranging from the ACLU to consumer groups to Phyllis Schlafly's Eagle Forum, supported more comprehensive privacy protection provisions proposed by a broadly bi-partisan group led by then-Rep. Ed Markey (D-MA) and Rep. Joe Barton (R-TX).[29]

The final law also required banks and certain non-banks, including consumer credit reporting firms, to comply with its data security provisions.[30]

Although the 2010 Dodd-Frank Act enacted in the wake of the 2008 financial collapse transferred authority to regulate credit reporting under FCRA to the tough new Consumer Financial Protection Bureau, its Section 1093 retained Title V data security provisions for non-banks under the weaker FTC. Unlike CFPB, that agency cannot supervise the activities of firms on a day-to-day basis, nor can it impose civil money penalties for a first violation.

The Congress Needs To Allow Consumers To Hold Firms More Accountable: In the immediate circumstance, the best way to give consumers protection against data breaches is to hold firms that lose our information accountable, including through their wallets. Threats to consumers can include fraud on existing accounts, new account identity theft, medical identity theft, tax refund identity theft and imposters committing crimes using your identity. Measurable harms from these misuses are obvious, but any measure of harms must also include the cost and time spent cleaning these problems up, additional problems caused by an empty checking account or a missing tax refund and being denied or paying more for credit or insurance or rejected for jobs due to the digital carnage caused by the thief. Consumers also face very real emotional stress and even trauma from financial distress. Breach harms also include the threat of physical harm to previous domestic violence victims.[31]

---

[27] "Defendants US Bank National Association ND and its parent holding company, US Bancorp, have sold their customers' private, confidential information to MemberWorks, Inc., a telemarketing company, for $4 million dollars plus commissions of 22 percent of net revenue on sales made by MemberWorks." Complaint filed by the State of Minnesota against U.S. Bank, 9 June 1999, available on Internet Archive, last visited 30 October 2017, https://web.archive.org/web/20010423055717/http://www.ag.state.mn.us:80/consumer/privacy/pr/pr_usbank_06091999.html

[28] The 1999 GLBA required annual privacy notices of financial institution information sharing practices and of the limited right to opt-out it provided. Industry organizations have relentlessly sought to eliminate the annual notice provisions. A transportation bill known as the FAST Act codified a narrowing of the requirement as a rider in 2015, as explained by the Consumer Financial Protection Bureau, https://www.federalregister.gov/documents/2016/07/11/2016-16132/annual-privacy-notice-requirement-under-the-gramm-leach-bliley-act-regulation-p HR 2396, We also oppose "The Privacy Notification Technical Clarification Act," to further narrow consumer rights to notice about privacy practices, was approved by this committee in a markup held on 11-12 October 2017, https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=402416

[29] The variety of groups that worked together for stronger privacy provisions is listed in this letter of 9 May 2000 to prudential regulators urging faster compliance of stronger rules, available on Internet Archive, last visited 30 October 2017, https://web.archive.org/web/20010425154255/http://www.pirg.org:80/consumer/glbdelay.htm

[30] The Federal Trade Commission's 2002 Safeguards Rule implements the law for non-bank "financial institutions, including the consumer reporting agencies and is available at https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule

[31] See Page 10, Testimony of Laura Moy, Deputy Director, Center on Privacy and Technology, Georgetown University Law Center, 25 October 2017, available at: https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-lmoy-20171025.pdf

II. Detailed Recommendations:

1) Congress should not enact any federal breach law that preempts stronger state breach notification laws or related protections:

In 2003, when Congress, in the FACT Act, amended the Fair Credit Reporting Act, it specifically did not preempt the right of the states to enact stronger data security and identity theft protections. We argued that since Congress hadn't solved all the problems, it shouldn't prevent the states from doing so.[32]

From 2004-today, nearly every state enacted security breach notification laws and enacted credit, or security, freeze laws. Many of these laws were based on the CLEAN Credit and Identity Theft Protection Model State Law[33] developed by Consumers Union and U.S. PIRG.

Congress should not preempt stronger state breach notification laws. **California** and **Texas**, for example, have very strong notification laws based on an ***acquisition*** standard. Information lost is presumed to be acquired, therefore requiring notice to breach victims. Industry actors would prefer use of a ***harm trigger*** before notice is required.

There are numerous problems with a harm trigger, which is a feature of some state laws and most proposed federal laws. The first is that the breached entity, which has already demonstrated extreme sloppiness with the personal information of its customers, gets to decide whether to inform them so that they can protect themselves.

The second problem is that industry groups would like any preemptive federal bill to define privacy harms very narrowly; their preferred bills would limit harms to direct financial harm due to identity theft.

Yet harms also include the cost and time spent cleaning these problems up, additional problems caused by an empty checking account or a missing tax refund and being denied or paying more for credit or insurance or rejected for jobs due to the digital carnage caused by the thief. Further, consumers face very real additional problems including the stigma of being branded a deadbeat and facing the emotional costs and worry that brings.

Only an acquisition standard will serve to force data collectors to protect the financial information of their trusted customers or accountholders well enough to avoid the costs, including to reputation, of a breach. Only if an entity's reputation is at risk will it do its best job to protect your reputation.

Further, as Laura Moy extensively pointed out at this committee's hearing last week, potential harms to consumers from misuse of information go well beyond financial identity theft.

> "In addition, trigger standards narrowly focused on financial harm ignore the many non-financial harms that can result from a data breach. For example, an individual could suffer harm to dignity if he stored embarrassing photos in the cloud and those photos were compromised. If an individual's personal email were compromised and private emails made public, she could suffer harm to her reputation. And in some

[32] For a detailed discussion of how the FACT Act left the states room to innovate, see Gail Hillebrand, "After the FACT Act: What States Can Still Do to Prevent Identity Theft," 13 January 2004, available at http://consumersunion.org/research/after-the-fact-act-what-states-can-still-do-to-prevent-identity-theft/

[33] U.S. PIRG and Consumers Union, "The Clean Credit and Identity Theft Protection Act: Model State Laws - A Project of the State Public Interest Research Groups and Consumers Union of U.S., Inc." Version of November 2005, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=846505

> circumstances, breach could even lead to physical harm. For example, the fact that a domestic violence victim had called a support hotline or attorney, if it fell into the wrong hands, could endanger her life."[34]

Ms. Moy's testimony is a magisterial analysis of the ways many broader state law protections would be eliminated by a narrow, preemptive federal bill. Bad outcomes she describes range from elimination of broad definitions of harms requiring notice and elimination of growing types of information protected by state laws (including **California, Florida, and Texas** laws requiring protection of physical and mental health records, medical history, and insurance information as well as elimination of a variety of state laws protecting online credentials, GPS data and biometric data). Ms. Moy also correctly urges the committee to leave the states room to respond to new, unknown threats.[35] Again, this is what the Congress did in the 2003 Fair and Accurate Transactions Act amendments to the FCRA, when it left the states free to respond to identity theft.

At that same hearing, **New York** Assistant Attorney General Kathleen McGee also notes that state notification laws have been expanded to include account credentials, biometric data and other protections. She also notes that nearly every state also holds firms accountable based on their consumer protection laws, which would also be preempted by many federal proposals.[36]

Other state attorneys general concur. As a news release accompanying **Illinois** Attorney General Lisa Madigan's recent testimony[37] to the U.S. Senate explained:

> "The Attorney General also testified that a federal data breach law must cover a broad range of sensitive data – not just social security numbers or stolen credit card numbers but also: online login credentials, medical information shared on the internet that is outside the scope of current privacy regulations, biometric data, and geolocation data. Companies must be required to report any data breach involving this type of personal information, Madigan said. Equally as important as Congress considers a federal data breach notification law, Madigan said, is the ability for state regulators to continue investigating data breaches at the state level. Federal legislation must not preempt the states' ability to respond and act when data breaches affect residents in their states. Any preemption by Congress must only provide a "floor" for reporting requirements and preserve a state's ability to use its consumer protection laws to investigate data security practices and enforce federal law.[38]

[34] See section 3, especially, of testimony of Laura Moy, Georgetown University Law Center's Center on Privacy and Technology, before this committee on 25 October 2017, available at https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-lmoy-20171025.pdf

[35] Testimony of Laura Moy, Georgetown University Law Center's Center on Privacy and Technology, before this committee on 25 October 2017, available at https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-lmoy-20171025.pdf

[36] Testimony of Kathleen McGee, Assistant Attorney General, Office of the New York Attorney General, at a hearing before this committee on 25 October 2017, available at https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-kmcgee-20171025.pdf

[37] "Getting it Right on Data Breach and Notification Legislation in the 114th Congress," A Hearing of the U.S. Senate Committee on Commerce, 5 February 2015, available at http://1.usa.gov/1tGFt5m

[38] Excerpt from news release: "Madigan: Federal Data Breach Law Should Not Weaken States' Consumer Protections", 5 February 2015, available at http://www.illinoisattorneygeneral.gov/pressroom/2015_02/20150205.html

General Madigan's office is also actively involved in the multi-state Equifax investigation, is calling for Equifax to pay for credit freezes for all Illinois residents and is supporting state legislation to provide free credit freezes.[39]

2) Congress Should Not Enact a Narrow, Preemptive Breach Law That Also Includes a Trojan Horse Provision to Preempt Broader State Data Security and Privacy Laws:

The other problem with enacting a preemptive federal breach notification law is that industry lobbyists will seek language that not only preempts state breach notification laws but also prevent states from enacting any future data security or privacy laws. This is the Trojan Horse problem. A small federal gain should not result in a big rollback of state authority.

As one example of a Trojan Horse provision I call your attention to a bill approved by this committee in the last Congress. HR 2205,[40] the Data Security Act of 2015 (Neugebauer), included sweeping preemption language that is unacceptable to consumer and privacy groups and likely also to most state attorneys general. While I note that this bill has numerous other objectionable provisions, which I am happy to discuss, its sweeping preemption language is illustrative of long-sought industry goals to take states off the board:

> SEC. 6. RELATION TO STATE LAW.
>
> No requirement or prohibition may be imposed under the laws, rules, or regulations of any State, the District of Columbia, or any territory of the United States with respect to the responsibilities of any person to--
>
> (1) protect the security of information relating to consumers that is maintained, communicated, or otherwise handled by, or on behalf of, the person;
>
> (2) safeguard information relating to consumers from--
>
> (A) unauthorized access; and
>
> (B) unauthorized acquisition;
>
> (3) investigate or provide notice of the unauthorized acquisition of, or access to, information relating to consumers, or the potential misuse of the information, for fraudulent, illegal, or other purposes;
>
> (4) mitigate any potential or actual loss or harm resulting from the unauthorized acquisition of, or access to, information relating to consumers.

Other bills before the Congress have included similar, if not even more sweeping, dismissals of our federal system. Such broad preemption will prevent states from acting as innovators of public policy or as first responders to emerging privacy threats. Congress should not preempt the states but instead always enact a floor of protection. In fact, Congress should think twice about whether a federal breach law that is weaker than the best state laws is needed at all. Congress should maintain co-authority of state Attorney General and other state and local enforcers; Congress should also retain state private rights of action, especially if it declines to create any federal private rights of action.

[39] News Release, 12 September 2017, available at http://www.illinoisattorneygeneral.gov/pressroom/2017_09/20170912.html

[40] HR 2205 is available at https://www.congress.gov/bill/114th-congress/house-bill/2205/

The testimony of Sara Cable, a **Massachusetts** Assistant Attorney General, before this committee, makes several points about the importance of state action abundantly clear:

> "The Equifax breach may bring into consideration whether a national data breach notice and data security standard is warranted. As noted, Massachusetts has among the strongest data security and breach laws in the country. My Office has serious concerns to the extent any federal standard seeks to set weaker standards that those that currently exist for Massachusetts consumers and that would preempt existing or future state law in this field. States are active, agile, and experienced enforcers of their consumers' data security and privacy, and need to continue to innovate as new risks emerge."[41]

Ms. Cable's testimony also notes Massachusetts Attorney General Maura Healey's strong support for free credit freeze legislation to be enacted by the state.

To the extent any national standard is considered by the committee, it must contain strong, minimum data security standards that do not erode existing state protections.

3) Congress Should Enact A Free Credit Freeze For All Law and Implement One-Stop Shopping for Freezes

Of course, I also believe that the minimum action Congress should take would be to extend free credit freezes at all 3 national consumer reporting agencies to all consumers at all times. The need for a free credit freeze to prevent identity theft was discussed in detail before the committee hearing last week by my colleague Mike Litt.[42] The committee should also ensure one-stop shopping for credit freezes, as is already the law for fraud alerts. You should need to contact only one credit bureau to gain protection at all three.

Mr. Litt's testimony also highlighted numerous other issues pertaining to how Equifax, Trans Union and Experian offer their own inferior packages of "locks" and other products that may force consumers to accept unfair terms and conditions with diminished rights and protections. Congress should also provide breach victims with an additional free credit from each national bureau.

4) The Congress Should Transfer Authority Over Gramm-Leach-Bliley Title V to the Consumer Bureau

We are encouraged that at the first Equifax hearing, that the full committee chairman, Mr. Hensarling, supported a review of the Gramm-Leach-Bliley framework, when he said "We must thoroughly examine if our agencies and statutes like Gramm, Leach, Bliley; the Fair Credit Reporting Act; and UDAAP [Unfair, Deceptive, Abusive Acts and Practices] are up to the job".[43]

We support, as did the National Consumer Law Center at last week's hearing, transferring Gramm-Leach-Bliley Title V responsibilities to the CFPB from the Federal Trade Commission. The FTC cannot impose civil penalties

---

[41] Testimony of Sara Cable, Assistant Attorney General, Office of the Massachusetts Attorney General, before this committee, 25 October 2017, available at https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-scable-20171025.pdf Note also that Ms. Cable references her earlier, more comprehensive testimony before the Congress for further details on the Massachusetts data security requirements.

[42] Testimony of Mike Litt, U.S. PIRG, before this committee, 25 October 2017, available at https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-mlitt-20171025.pdf

[43] Opening statement of Financial Services Committee Chairman Jeb Hensarling, 5 October 2017, available at: https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=402391.

for a first violation of the rules; it can only impose penalties after an enforcement order is violated. The FTC has no authority to supervise firms, as the Consumer Bureau does. The Consumer Bureau has much broader rulemaking authority than the FTC.

5) Congress Should Enact Comprehensive FCRA Reforms, H.R. 3755, the Comprehensive Consumer Credit Reporting Reform Act (Waters) and Also Protect the Consumer Bureau

I first testified in favor of Fair Credit Reporting Act reform in 1989, before a predecessor subcommittee of the old House Banking Committee called Consumer Affairs and Coinage. While credit bureau reform has been a work in progress ever since then, we made major strides in 1996 and 2003. Then, with the establishment of the Consumer Bureau in 2010, which began supervising the larger bureaus in 2012, we have seen more advances. I concur with the detailed testimony by Chi Chi Wu on numerous occasions in support of further legislative reforms and urge the committee to pass HR 3755 as proposed by Ranking Member Waters. As Chi Chi Wu said to the full committee last week:

> "Due to this insufficient regulation and the lack of consumer choice, the credit reporting agencies have grown up in a culture of impunity, arrogance, and exploitation. For decades, they have abused consumers, cut corners in personnel and systems, and failed to invest in measures that would promote accuracy or handle disputes properly."[44]

We concur. We also urge reconsideration of the majority's views on the Consumer Bureau. It has done yeomen work for consumers, while being fully transparent in its efforts. It is needed now, more than ever.

6) Congress Should Allow Private Enforcement and Broad State and Local Enforcement of Any Law It Passes: The marketplace only works when we have strong federal laws and strong federal enforcement of those laws, buttressed by strong state and local and private enforcement.

Virtually all federal privacy or data security or data breach proposals specifically state that no private right of action is created. Such clauses should be eliminated and it should also be made clearer that the bills have no effect on any of the 17 state law private rights of action that apply to data security and breaches. Further, no bill should include language reducing the scope of state Attorney General or other state-level public official enforcement. Further, any federal law should not restrict state enforcement only to state Attorneys General, but allow enforcement by local enforcers, such as district attorneys.

7) Congress Should Address SSNs and authentication:

In the U.S., new account identity theft and other frauds, including tax refund fraud and medical services fraud, are fueled both by the high demand for "instant credit" and by that critical flaw in our credit granting system, where SSNs serve as both a matching identifier in databases and as an authenticator of a consumer applicant. The Social Security Number genie left the bottle years ago. While we would prefer that it not be used as a commercial identifier, in numerous databases, it is. The Congress needs to examine how to prevent it from being used as both an authenticator and an identifier. Your ATM card PIN is a secret authenticator. It is different from your bank account number and known only to you. Whether it is a two-factor authentication or some other solution, we need

[44] Testimony of Chi Chi Wu, National Consumer Law Center, before the committee on 25 October 2017, available at https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-ccwu-20171025.pdf

to move on from using Social Security Numbers for both identification and authentication because SSNs are not secret and don't do the job.[45]

8) Congress should further investigate marketing of overpriced credit monitoring and identity theft subscription products:

Prices for credit monitoring, credit scoring and identity theft protection and remediation products from credit bureaus, banks and firms such as Lifelock range up to $19.99/month or more. The marketing of the products, often based on scant 3-5 day free trial periods, is often deceptive. In 2017, the Consumer Bureau imposed fines totaling over $23 million on both Equifax and Transunion over their marketing of credit scores and subscription credit monitoring services.[46]

In 2005 and then again in 2007 the FTC had imposed a total of over $1.2 million in fines on the credit bureau Experian's subsidiary Consumerinfo.com for deceptive marketing of its own various credit monitoring products; Experian had tied its expensive subscription product to the new free annual credit report required by law.[47]

Banks receive massive commissions for selling these under-performing, over-priced products to their own customers. The Consumer Bureau has also imposed fines totaling about $1.5 billion on big banks selling similar products, derived from consumer credit reporting products. While it is likely that those Consumer Bureau enforcement orders[48] against several large credit card companies for deceptive sale of the add-on products has caused banks to think twice about continuing these relationships with third-party firms, the committee should also consider its own examination of the sale of these credit card add-on products.

Lifelock, a major company in the identity protection space, was fined $12 million in 2010 by the FTC and 35 states for deceptive marketing.[49]
Then, in 2015, the FTC held Lifelock in contempt and fined it an additional $100 million for failing to protect the security of its customers' files and falsely advertising that it had.[50]

In his testimony before Congress, Richard Smith of Equifax admitted that Lifelock was a third-party partner of

[45] See "Security In Numbers: SSNs and Identity Theft," an FTC report, which discusses the problems of using Social Security Numbers to authenticate people even though they are not secret, but ubiquitous and widely available to thieves, December 2008, available at https://www.ftc.gov/sites/default/files/documents/reports/security-numbers-social-security-numbers-and-identity-theft-federal-trade-commission-report/p075414ssnreport.pdf

[46] Press release, "CFPB Orders TransUnion and Equifax to Pay for Deceiving Consumers in Marketing Credit Scores and Credit Products," 3 January 2017, available at https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-transunion-and-equifax-pay-deceiving-consumers-marketing-credit-scores-and-credit-products/

[47] Press release, "FTC Alleges Ads For "Free" Credit Report Violate Federal Court Order," 21 February 2007, available at https://www.ftc.gov/news-events/press-releases/2007/02/consumerinfocom-settles-ftc-charges

[48] We discuss some of the CFPB add-on cases against bank marketing of subscription products here https://uspirg.org/blogs/eds-blog/usp/cfpb-gets-results-consumersand-taxpayers-too

[49] Press release, "LifeLock Will Pay $12 Million to Settle Charges by the FTC and 35 States That Identity Theft Prevention and Data Security Claims Were False," 9 march 2010, available at https://www.ftc.gov/news-events/press-releases/2010/03/lifelock-will-pay-12-million-settle-charges-ftc-35-states

[50] "LifeLock to Pay $100 Million to Consumers to Settle FTC Charges It Violated 2010 Order," 12 December 2017, available at https://www.ftc.gov/news-events/press-releases/2015/12/lifelock-pay-100-million-consumers-settle-ftc-charges-it-violated

the credit bureau.[51]

Consumers who want credit monitoring can monitor their credit themselves. No one should pay for it. You have the right under federal law to look at each of your 3 credit reports (Equifax, Experian and TransUnion) once a year for free at the federally-mandated central site annualcreditreport.com. Don't like websites? You can also access your federal free report rights by phone or email. You can stagger these requests – 1 every 4 months -- for a type of do-it- yourself no-cost monitoring. And, if you suspect you are a victim of identity theft, you can call each bureau directly for an additional free credit report. If you live in Colorado, Georgia, Massachusetts, Maryland, Maine, New Jersey, Puerto Rico or Vermont, you are eligible for yet another free report annually under state law by calling each of the Big 3 credit bureaus.

9) Any federal breach standard should not treat merchants differently than financial institutions:

Nearly every federal breach notification bill that requires breach notification by covered entities (regardless of its harm trigger or other provisions), seeks to provide a safe harbor to entities already covered by Title V of the Gramm-Leach-Bliley Act or other federal data security laws, such as those applicable to health care entities.[52] As merchants and retailers have long pointed out, this leaves them, as non-financial institutions under the GLBA scheme, subject to notification standards higher than those of GLBA "financial institutions." Such a two-tiered system makes no sense from a policy perspective. Of course, merchants have also suffered enmity from banks and credit unions which seek affirmative legislation holding them liable for breach costs. Such disputes should be covered in contract, not law.

III. Conclusion: A Threat to Consumers Is Posed by the Basic Business Model of the Digital Data Advertising Ecosystem

This testimony focuses primarily on the impact of a failure to secure consumer information. Congress should also investigate the broader problem of the over-collection of consumer information for marketing, tracking and predictive purposes. While the digital advertising ecosystem expands the number of vectors for misuse, the ubiquitous tracking of consumers as commodities or products poses threats as a business model itself.[53]

In many ways, data breaches are the mere tip of the iceberg when it comes to privacy threats in the Big Data world. In the Big Data world, companies are collecting vast troves of information about consumers. Every day, the collection and use of consumer information in a virtually unregulated marketplace is exploding. New technologies allow a web of interconnected businesses – many of which the consumer has never heard of – to assimilate and share consumer data in real-time for a variety of purposes that the consumer may be unaware of and may cause consumer harm. Increasingly, the information is being collected in the mobile marketplace and includes a new level of hyper-localized information.

Contrast the FCRA with the new Big Data uses of information which may not be fully regulated by the FCRA. The development of the Internet marketing ecosystem, populated by a variety of data brokers, advertising

[51] Tara Siegel Bernard, "The Post-Equifax Marketing Push: Identity Protection Services," 25 October 2017, available at https://www.nytimes.com/2017/10/25/your-money/identity-protection-equifax.html
[52] See the Health Insurance Portability and Accountability Act (HIPAA) (45 CFR Subpart C of Part 164).
[53] See Edmund Mierzwinski and Jeff Chester, "Selling Consumers, Not Lists: The New World of Digital Decision-Making and the Role of the Fair Credit Reporting Act," 46 Suffolk University Law Review Vol. 3, page 845 (2013), available at http://suffolklawreview.org/wp-content/uploads/2014/01/Mierzwinksi-Chester_Lead.pdf

networks and other firms that collect, buy and sell consumer information without their knowledge and consent, is worthy of much greater Congressional inquiry.[54] As I wrote, with a colleague from the Center for Digital Democracy:

> "Dramatic changes are transforming the U.S. financial marketplace. Far-reaching capabilities of "Big-Data" processing that gather, analyze, predict, and make instantaneous decisions about an individual; technological innovation spurring new and competitive financial products; the rapid adoption of the mobile phone as the principal online device; and advances in e-commerce and marketing that change the way we shop and buy, are creating a new landscape that holds both potential promise and risks for economically vulnerable Americans."[55]

Conclusion:

Congress has largely failed to address numerous digital threats to consumers, from data breaches to data brokers running amok to the very architecture of the digital ecosystem, where nearly every company -- known and unknown – is tracking consumers, building a dossier on them and even auctioning them off to the highest bidder in real time (for advertising or financial offers). Any data security, breach or privacy legislation should provide individuals with meaningful and enforceable control over the collection, use and sharing of their personal information.

Any bill should become a federal floor that upholds state privacy and data security laws, grants strong regulatory and enforcement authority to the Federal Trade Commission and state officials and allows states to continue to act as privacy leaders. Congress should give the Federal Trade Commission (FTC) adequate resources to protect privacy. Congress should defend the Consumer Bureau.

Any bill should adequately define what constitutes sensitive information, and provide consumers with meaningful choices about use of their data (ideally an opt-in to any secondary use). Any bill should protect large categories of personal information, including geolocation data, health records and marketing data collected on or off line. There should be no exceptions for business records, data "generally available to the public," and cyber threat indicators.

Proposed bills should not give companies leeway to determine the protections that consumers will receive. Most proposed bills' protections apply only if a company identifies a "context" or risk of harm. Protections should not be conditioned in such a way. Companies should face the threat of public exposure for failing to protect customer information. Companies should face monetary penalties to victims.

As Congress considers amendments to address all the issues highlighted in this testimony, from data breaches to data security to data brokers and the Internet advertising ecosystem, it needs to consider any reforms in the context of the strongest possible application of the Code of Fair Information Practices discussed above.

---

[54] See the FTC's March 2012 report, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers," available at https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/ftc-privacy-report

[55] Edmund Mierzwinski and Jeff Chester, "Big Data Means Big Opportunities and Big Challenges," 27 March 2014, U.S. PIRG and the Center for Digital Democracy, available at https://uspirg.org/reports/usf/big-data-means-big-opportunities-and-big-challenges

It is important that policymakers understand that you cannot bifurcate the issues of data security and privacy. Consumer privacy is threatened when companies can buy or sell our information and we have little choice or control. Consumer privacy is threatened when data collectors do not keep data secure. In the new Big Data world, where firms are racing to vacuum up even more data than ever before, with even less acknowledgement of any privacy interest by consumers (or citizens), it is important that we re-establish norms that give consumers and citizens greater control over the collection, and use, of their personal information.

Thank you for the opportunity to provide the Committee with our views. We are happy to provide additional information to Members or staff.

—