Testimony of Edmund Mierzwinski,

U.S. PIRG Consumer Program Director

Hearing on "Identity Verification In A Post-Breach World"

Before the House Committee on Energy and Commerce,

Subcommittee on

Oversight and Investigations

Honorable Tim Murphy, Chair

30 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 Murphy, Representative DeGette, 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:

I appreciate that the committee is holding an oversight hearing on approaches to improving identity verification. It is important to review the best ways to move past the use of obsolete authentication systems that rely on social security numbers. You cannot authenticate with a number that is also an identifier, especially one that anyone can obtain, thanks to the data breach world we live in. Further, I am not sure so-called knowledge-based authentication was ever adequate, when it has often relied on a series of somewhat predictable questions. The problem has now worsened when any imposter can obtain most answers in real-time searches and, worse, when most actual consumers are asked truly stupid questions. Simply to place a credit freeze, my colleague had to try to explain to Equifax, after its well-publicized and ongoing debacle, that "No, Chester doesn't co-own any property with me or have any credit cards. He was my dog when I was 5 years old and he died a long time ago." And how many times has your student loan servicer changed names or changed hands? Is it Sally Mae or Navient? How do you answer?

My testimony also discusses that data breach responses need a careful approach by Congress. The authoritative Privacy Rights Clearinghouse has estimated that at least 10,057,873,432 records have been breached in a total of at least 7,831 data breach occurrences made public since 2005.[1] The massive exploit against Equifax, a major consumer credit reporting agency (colloquially, a credit bureau), not only affected at least 145.5 million

[1] See Data Breach page at Privacy Rights Clearinghouse, last visited 28 November 2017, https://www.privacyrights.org/.

consumers, but compromised perhaps the richest trove of personal information I have seen in my over 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. Meanwhile, Uber has finally reported the breach, in 2016, of some 57 million consumer and driver profiles.

I believe that multi-factor authentication is part of the solution. One factor might be something secret that only "you know," such as a password, but certainly not your SSN. Another might be something "you have," such as a phone or computer that can receive a verification text. A third might be something "you are," such as your fingerprint or retina scan.

I do, however want to point out that the privacy and civil liberties communities are concerning about some of the implications of biometric identifiers. I am quite happy to have the convenience of a fingerprint passcode on my computer and cell phone, but only if they remain encrypted on those devices and are not made part of some larger, hackable database in the cloud and/or available to the government.

I also want to make the point that, like clockwork, after any big data breach is disclosed, powerful special interests seek to turn the problem into a bigger problem for consumers by using it as an opportunity to enact some sort of narrow federal legislation that broadly eliminates state data breach notification, state data security and other privacy protections. Industry lobbyists routinely mask their Trojan Horse efforts behind a "fix the patchwork, balkanized notice system" narrative to hide their broader plans. They don't simply want to create a

[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

"uniform national breach law." Inside that Trojan Horse is their ultimate plan: to permanently take away all existing state data security laws and deny the states any authority to enact new privacy laws, even on new problems identified that Congress hasn't yet or purposely didn't solve.

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, any federal law to address the issues before this committee today should not endorse specific solutions that limit innovation or perpetuate oligopoly.

1) The Flaws of Authentication Based on Ubiquitous SSNs and Hackable Knowledge Based Authentication and Possible Solutions

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 already is. The Congress needs to examine how to prevent it from being used as both an authenticator and an identifier. As a simple explanation, 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 to move on from using Social Security Numbers for both identification and authentication because SSNs are not secret and don't do the job.[5]

As stated in the committee's majority staff hearing memo: "Given that much of modern commerce relies on a process of remote identity verification known as knowledge-based authentication or KBA, through which individuals prove who they are by answers to series of questions to which only they – in theory -- should know the correct responses, this ability to "package" identity information raises even more significant questions about the reliability of traditional KBA practices. […] With the wide-spread use of social media, consumer's unique identifiers for static KBA, are often available to the public [including] malicious actors."

I certainly agree that to rely on either static or dynamic KBA is to rely on an obsolete system. In addition to the ubiquity of much personal relationship information, easily available in one-second, real-time searches, much of the information remains a mystery to the consumer: "What lender originally held my student loan or mortgage?" It is likely that loan has been serviced more than once, or that the lender has changed its name at least once—from Sallie Mae to Navient, for example. My favorite recent example is the experience of one of my co-workers who tried to place a credit freeze on her Equifax credit report following their public announced of their debacle. Her s "security" question generated by Equifax was "Where did Chester [Last Name] have credit cards when you lived with him?" Her answer: "I was 5 years old and Chester was my dog and he died a long time ago." But that simply generated another question from Equifax.

A) Multi-Factor Authentication

I believe that multi-factor authentication is part of the solution. One factor might be something secret that only "you know," such as a password, but certainly not your SSN. Another might be something "you have," such as a phone or computer that can receive a verification text. A third factor under consideration might be something

[5] 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

"you are," such as your fingerprint or retina scan.

I do, however want to point out that the privacy and civil liberties communities are concerning about some of the implications of such biometric identifiers. As a simple example, I am quite happy to have the convenience of a fingerprint passcode on my computer and cell phone, but only if they remain encrypted on those devices and are not made part of some larger, hackable database copied to the cloud. As the authoritative Electronic Frontier Foundation has pointed out:

> Biometric identifiers include fingerprints; iris, face and palm prints; gait; voice; and DNA, among others. The government insists that biometrics databases can be used effectively for border security, to verify employment, to identify criminals, and to combat terrorism. Private companies argue biometrics can enhance our lives by helping us to identify our friends more easily and by allowing us access to places, products, and services more quickly and accurately. **But the privacy risks that accompany biometrics databases are extreme.** (Emphasis added).[6]

B: NIST in U.S. Government, Private Consortium FIDO Seek Trusted Identities

In an ongoing project, the U.S. government's National Institute on Standards and Technology has done multi-stakeholder research into development of principles for a new paradigm to develop online trusted identities to ensure that: "Individuals and organizations employ secure, efficient, easy-to-use, and interoperable identity solutions to access online services in a manner that promotes confidence, privacy, choice, and innovation."

NIST's project describes the principles of confidence, privacy, choice, and innovation in this way:

> "Identity solutions will be: privacy-enhancing and voluntary; secure and resilient; interoperable and cost-effective and easy to use."[7]

[6] The Electronic Frontier Foundation, Biometrics Issues, undated resources webpage available at https://www.eff.org/issues/biometrics

[7] Trusted Identities Group, "Overview: Building partnerships to advance digital identity," undated webpage available at https://www.nist.gov/itl/tig/about/overview

This project appears to have undertaken numerous pilot projects and partnerships. Its output is worthy of further review.

In the private sector, the Fast Identity Online Authentication (FIDO) Alliance[8] is a 4-year-old international consortium seeking to replace the use of passwords with public-key encryption based multi-factor authentication. While I have not had the opportunity to examine it in detail, it appears to rely on an open standard and an open standard-setting setting process.

In my view, any project that the Congress endorses must rely on open, technology-neutral, technology-forcing performance standards and not memorialize any specific way of achieving them, which could become obsolete, into law.

C. Closed Standards Don't Work

Contrast the apparent openness of the FIDO approach with the oligopolistic Payment Card Standards (PCS) system that the card networks and the banks impose on merchants that seek to accept credit and debit cards.[9] While the banks and card networks have largely blamed merchants (Home Depot, Target, Michael's Stores, Barnes & Noble, etc.) for a series of massive merchant breaches, the real problem was always the card networks' insistence on over-extending the lifespan of obsolete magnetic-stripe cards, which the merchants were forced to accept. Then, when they finally announced the so-called EMV transition, the networks chose the partial solution of switching to Chip, rather than Chip and PIN cards, which had already been in use in many countries for years. The oligopolists chose to advance not to the "current best available technology," but only to "the best available technology that helps maintain profits and locks out would-be competitors." While a Chip card used in a card-present transaction proves your card is not a clone and scrambles a one-time use number so card numbers are not

[8] Fact Sheet, "What Is FIDO?," undated, available at https://fidoalliance.org/about/what-is-fido/
[9] Wikipedia, "Payment Card Industry Data Security Standard Page," October 2017, available at https://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard,"

retained in merchant systems, a PIN-requirement would also prove that the user is not an imposter.[10]

Of course, the rollout of Chip cards has reduced card-present fraud, but caused fraudsters to move to online scams. This predictable result, however, has also hastened the development of better online transaction security systems. In fact, some of the best new online security methods include services allowing the use of a PIN to protect against fraud online.[11]

2) Equifax and Other Breaches:

A. Equifax, A Huge Warning; The Uber Breach, A Nagging Reminder:

I remain incredulous that Equifax, a data broker with only one job -- buying and selling consumer information -- had such an epic fail in protecting that information and then responded badly to its epic fail. I commend the bi-partisan Energy and Commerce committee leadership for persistently demanding further information from this recalcitrant wrongdoer.[12]

The Equifax breach was among the worst ever because the firm lost your financial DNA. Your Social Security Number is the key to identity theft: it doesn't change and may become more valuable to thieves over time, unlike a merchant breach of a credit card number, which has a limited shelf life.

Yes, Equifax is a highly-regulated credit bureau. But its larger business is as a largely unregulated data broker. In the broad data broker and Big Data universes consumers have no rights to control the collection and sale of their personal information. We are products, not customers. 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

[10] See my testimony before the House Committee on Small Business, "The EMV Deadline and What it Means for Small Businesses: Part II," 21 October 2015, available at https://smallbusiness.house.gov/uploadedfiles/10-21-2015_mierzwinski_testimony.pdf

[11] For illustrative purposes, not endorsement, you can see video demos for this service by Acculynk (now owned by First Data) available at http://acculynk.com/resource/list/1

[12] Letter from Chairman Greg Walden, Subcommittee Chairman Bob Latta, Ranking Member Frank Pallone and Subcommittee Ranking Member Jan Schakowsky to Equifax Interim CEO Paulino do Rego Barros, Jr., and Equifax Chairman Mark Feidler, 17 November 2017, available at https://energycommerce.house.gov/news/press-release/committee-leaders-continue-push-equifax-data-breach-details/

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)[13] 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 several other Congressional hearings.[14]

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 it's the bank or other creditor, which is a trusted third party (and likely answers no security questions) and has easy access to the credit reporting company, that 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.[15]

B. Worse, Equifax Is 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

[13] 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/
[14] 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
[15] 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

provider or government agency. Incredibly, this is not the first security problem Equifax has faced recently.[16]

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.

The Equifax breach extensively reviewed in numerous Congressional 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);[17] 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.).[18] 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.

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:[19]

---

[16] 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

[17] 15 U.S.C. 1681 *et seq.*

[18] 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

[19] 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

> "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:[20] "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:[21] "The power behind our solutions—and your acquisition programs—is the superior quality of our data."
- The data broker Transunion:[22] "TransUnion offers more complete and multidimensional information for informed decisions that create opportunities for your business."

C. Privacy Laws Need to Be Based on Fair Information Practices

[20] http://www.experian.com/business-services/business-services.html
[21] http://www.equifax.com/business/acquire-more-customers
[22] https://www.transunion.com/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,[23] 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 1974 U.S. Privacy Act and governs information use by federal agencies.[24] 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.[25]"

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

[23] "…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

[24] "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

[25] 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

compensation) against the infringing company. Importantly, the GDPR, when it goes into final effect next year, trumps the existing Privacy Shield[26] 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.[27] The GDPR would also subject firms to civil penalties for failing to report data breaches.[28] We support, as does the National Consumer Law Center, transferring Gramm-Leach-Bliley Title V responsibilities to the CFPB from the Federal Trade Commission. The FTC cannot impose civil penalties 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.

Paradox: Identity theft is 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."[29] Estimates are that consumers spend at least $3 billion/year on credit monitoring services.[30]

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.[31]

---

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

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

[28] Nina Trentmann, "Data Breaches Will Soon Cost Companies in Europe," the Wall Street Journal, 22 November 2017, available at https://www.wsj.com/articles/data-breaches-will-soon-cost-companies-in-europe-1511386000

[29] 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

[30] 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/

[31] On 7 September 2017, the date that the Equifax breach was announced to the public, the Financial Services 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

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.[32] Lifelock has been fined both for unfair marketing and contempt ($100 million) when it failed to comply with an FTC order.[33]

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.

Paradox: Businesses are customers and consumers are 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, first director of the Consumer Financial Protection Bureau, often calls credit reporting one of several "dead-end

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

[32] 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/

[33] Press release, "Lifelock Fined $100 Million for Contempt," 17 December 2015, available at https://www.ftc.gov/news-events/press-releases/2015/12/lifelock-pay-100-million-consumers-settle-ftc-charges-it-violated

markets" in need of stricter regulation to counter that market failure.[34]

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.[35] Nevertheless, we are encouraged by the recent efforts by the Consumer Bureau to achieve changes to the Big 3's operations through supervision.[36]

D. 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, which was sued by the State of Minnesota for sharing customer records with a third-party telemarketer that then preyed on its customers,[37] 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).[38] A wide variety of organizations, ranging from the ACLU to consumer groups to Phyllis Schlafly's Eagle Forum, supported more comprehensive privacy protection provisions

[34] 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/

[35] 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

[36] 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

[37] "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

[38] 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

approved in this committee as proposed by a broadly bi-partisan group led by then-Rep./now Sen. Ed Markey (D-MA) and Rep. Joe Barton (R-TX).[39] The final law also required banks and certain non-banks, including consumer credit reporting firms, to comply with its data security provisions.[40]

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.

D. Don't Forget the Uber Breach

Then came the Uber breach. Mr. Pallone, the full committee ranking member, has rightly urged an investigation. Some 600,000 drivers had their financial DNA taken. While the information of over 56 million consumers that was also breached was apparently limited to names, email addresses and phone numbers subject to social engineering phone calls and "phishing" emails, the announcement of the Uber breach, hard on the heels of the Equifax breach, should serve as a reminder that until we do something, breaches will continue. Of course, Mr. Pallone's request for an investigation also points out that Uber, as many breached entities before it, chose to ignore clear state laws requiring prompt notification to victims and also, in many states, to law enforcement officials, when it waited over a year to notify anyone. Worse, of course, Congress needs to get to the bottom of its apparently paying a ransom to the thieves to keep it quiet for their own business development purposes. I would also ask Uber what proof it has that thieves would actually give back their only copy of stolen information, even if a ransom were paid.

3) Recommendations:

[39] 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

[40] 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

A. Congress Must Reject Industry Trojan Horses Seeking State Preemption:

I cannot overstate the political conundrum that although the severity of the Equifax breach and the relentless march through the headlines of other breaches demand that policymakers enact stronger, not weaker, consumer protections, Congress instead often considers industry-backed bills to preempt, or override, numerous stronger state data breach and data security protections. Worse, the bills have a kicker: most permanently take the states off the board as privacy first responders and innovators.

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 HR 1770, the Data Security and Breach Notification Act of 2015, a bill approved by this committee in the last Congress. The bill included sweeping data security and data notification 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 – historically privacy leaders -- off the privacy board.

Of course, this committee's Trojan Horse preemption language was not as sweeping as one in a bill approved by the Financial Services Committee in the last Congress. HR 2205,[41] the Data Security Act of 2015 (Neugebauer), included even more sweeping preemption language. (Section 6).

Numerous critical provisions of California, Massachusetts, Illinois, Texas and other state breach notification laws could be eliminated as would 17 state laws that include a consumer private right of action to sue data breach notification law violators. I urge the committee not to preempt state privacy laws. Instead, focus on proposals that return some control over their personal information to consumers, such as widely supported proposals to allow consumers to place and lift credit freezes on their credit reports for free. While that action may not be squarely in the committee's ambit, it is the best narrow, do-able response to the breach debacle.

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

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.[42]

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[43] 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

[42] 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/

[43] 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

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 has extensively pointed out to this and other committee, potential harms to consumers from misuse of information go well beyond financial identity theft to harm to dignity reputation and even physical harm.[44] 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 Congress to leave the states room to respond to new, unknown threats.[45]

New York Assistant Attorney General Kathleen McGee has recently suggested to Congress that state notification laws have been expanded to include protection 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.[46]

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.

---

[44] 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

[45] 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

[46] 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

The most recent testimony of Sara Cable, a **Massachusetts** Assistant Attorney General, who has previously appeared before this committee, made 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."[47]

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 notification standard is considered by the Congress, it must contain strong, minimum data security standards that do not erode existing state protections.

Other state attorneys general including **Illinois** Attorney General Lisa Madigan, concur.[48] 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.[49]

No GLBA Safe Harbor: Nearly every federal breach notification bill that requires breach notification by covered entities (regardless of its harm trigger or other provisions), also 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.[50] 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

[47] 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.
[48] "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
[49] News Release, 12 September 2017, available at http://www.illinoisattorneygeneral.gov/pressroom/2017_09/20170912.html
[50] See the Health Insurance Portability and Accountability Act (HIPAA) (45 CFR Subpart C of Part 164).

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.

B. Congress Should Allow Consumers to Hold Breached Firms Accountable In Court

In the immediate circumstance, the best way to give consumers protection against data breaches is to let us 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.[51] Congress must main private rights of action against corporate wrongdoers.

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.

C. Congress Should Enact A Free Credit Freeze For All Law and Implement One-Stop Shopping for Freezes and also Consider Making the Freeze an Always-On Default

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 Congress should also ensure one-stop

[51] 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

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.

While we support the credit freeze as a minimum, a next step, once radical but now worthy of discussion, would be to make the credit freeze the always-on default. Consumer DNA should always be frozen; freezes should only be lifted at the consumer's request.

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

We support, as does the National Consumer Law Center, transferring Gramm-Leach-Bliley Title V responsibilities to the CFPB from the Federal Trade Commission. The FTC cannot impose civil penalties 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.

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.[52]

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

[52] 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

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 networks and other firms that collect, buy and sell consumer information without their knowledge and consent, is worthy of much greater Congressional inquiry.[53] As I wrote, with a colleague from the Center for Digital Democracy:

[53] 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

> "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."[54]

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.

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.

I appreciate the committee's thoughtful approach in taking a closer look at ways to improve online authentication of consumers and for the opportunity to provide the Committee with our views. We are happy to provide additional information to Members or staff.

—

[54] 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