

Testimony of Edmund Mierzwinski
U.S. PIRG Consumer Program Director

at a hearing on

**“Cybersecurity: The Evolving Nature of
Cyber Threats Facing the Private Sector”**

Before the House Committee on Oversight and Government Reform
Subcommittee on Information Technology
Honorable William Hurd, Chair

18 March 2015

**Testimony of Edmund Mierzwinski, U.S. PIRG Consumer Program Director at a hearing
on “Cybersecurity: The Evolving Nature of Cyber Threats Facing the Private Sector”
House Subcommittee on Information Technology, 18 March 2015**

Chairman Hurd, Representative Kelly, members of the committee, I appreciate the opportunity to testify before you on the important matter of cyber threats, which I construe broadly in this testimony to include not only data breaches but also generally accepted industry practices that may actually be unfair to consumers. 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:

The authoritative Privacy Rights Clearinghouse has estimated that since 2005, at least 815,842,526 records have been breached in a total of at least 4,495 data breach occurrences made public since 2005.¹ One of the latest exploits, against Anthem, a health insurance company, not only affected up to 80 million consumers, but compromised among the richest troves of personal information I have seen in my 25 years of privacy research.

Data collectors collect and save too much information on consumers, keep it too long and often use it without consumer knowledge, let alone permission. While consumer and privacy organizations believe we need a robust Consumer Privacy Bill of Rights, based on a strong version of the Code of Fair Information Practices, in the short run we need to address the failure of data collectors – including retailers, banks, universities, government agencies, health insurers and others – to protect customer information from misuse. Data breaches, hacks and misuse cost the economy billions of dollars and cause profound harms to consumers.

It is important that policymakers understand that you cannot bifurcate the issues of data security and privacy. 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.

In the immediate circumstance, the best way to give consumers protection against data breaches is to hold firms that lose their information accountable. 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

¹ See “Chronology of Data Breaches,” Privacy Rights Clearinghouse, last visited 15 March 2015, <https://www.privacyrights.org/data-breach>.

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.

Cyber security problems are caused by a variety of factors. Banks blame merchants for shoddy card security. While banks expect merchants to build higher cyber walls every year, only recently have they begrudgingly begun to take steps to phase out their obsolete, reckless 40-year old magnetic stripe credit and debit card technologies. Even now, however, the banks would prefer to move only incrementally, to Chip and Signature cards, even though a more secure technology, Chip and PIN, has been around for years in other countries. The Chip ensures that your card is not a clone; the PIN ensures that you are not an imposter. Nevertheless, policymakers should embrace neither technology, but should take steps to urge firms to use the best-available technology-neutral technologies. Of course, these card changes only will reduce retail point-of-sale fraud; the threat of card-not-present fraud (such as Internet purchases) requires additional improvements.

In my testimony, I will discuss these and other issues that our failure to enforce adequate data security has on consumers. I rely on the other witnesses today to explain the problems banks, merchants and other firms face. On some matters, we may even agree. 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. Some Breaches Involve Card Numbers, Others Are Worse

It is important to understand that not all breaches are created equal. Here is a rough hierarchy, in ascending order of harm to consumers.

1) Card Number Breach: When merchant terminals are breached, typically the only information stolen is credit and debit card numbers. These numbers can only be used for what is called existing account fraud. While this costs the banks or merchants money, consumers are generally well-protected by law from bearing the costs of any frauds. Credit card fraud liability is limited by law to \$50; debit card liability is zero if the consumer notifies the institution within 60 days (when only the number, but not the device) is stolen.² In the case of debit cards, of course, the consumer may face the additional problem of bouncing other checks until the bank returns her money to her account. That is why every consumer advocate I know recommends that consumers who can avoid the temptation of carrying credit card debt only use credit cards at

² Debit card liability is much higher if the card is stolen, and liability increases dramatically after 60 days. <http://www.uspirgedfund.org/news/usp/groups-offer-consumer-tips-after-target-data-breach> (last visited 3 March 2015).

retail or online. Unfortunately, however, only a very small number of banks and credit unions offer PIN-only ATM cards; nearly all only offer “debit cards” that can be used at ATMs with a PIN but also at point of sale with just a swipe and signature.

2) Phishing, When General Customer Information (email/phone/address) also Breached:

Obtaining a consumer’s email address allows the thief to make “phishing” attacks, hoping the consumer will click a link that allows a virus to invade her computer and obtain more information – such as bank account passwords, or Social Security Numbers, etc. Obtaining a phone number associated with a known bank or other account allows the thief to make “social engineering” phone calls, hoping to use the small amount of information that they have to trick the consumer into giving up more. Spear-phishing is a more sophisticated variant where the thief is looking for targeted information from employees of certain companies or agencies, for the secondary purpose of industrial, or state-sponsored, espionage.

The additional information the bad guys seek, then, would either allow them direct access to your existing account (through the PIN or credit card security code (CVV) that they didn’t have before) or to open new accounts in your name (with your Social Security Number) by committing identity theft. They use what they know to convince you to tell them what they don’t know. They want your PIN, or your birthdate or Social Security Number. They hope to trick you into giving it up.

3) Social Security Numbers and other Details Breached: The Social Security Number is the key that unlocks your credit report and tax refund. Armed with a social security number, a thief can apply for new accounts in your name. The thief doesn’t breach your report. He provides a creditor with an application containing your Social Security Number but his address. Such financial identity theft lowers your credit score, causing you to be denied credit or jobs. Cleaning up financial identity theft can be a nightmare for consumers, despite a number of changes that were made to the Fair Credit Reporting Act in 2003.

Worse, convincing the IRS that a thief obtained your tax refund before you were able to file is similarly a nightmare for consumers that takes 3-6 months or more to clean up (and only then obtain your refund). While Intuit TurboTax continues to deny that it was breached in a recent incident involving thousands of state returns, not only do security experts³ contend that the firm failed to use best practices to verify taxpayer identities but state tax officials⁴ also argue that it failed to respond to their warnings. As the Washington Post explained:

³ Brian Krebs argues that Intuit not only did not use email and phone validation, it did not confirm account changes with customers or use “Know-Your-Customer” validation (until after the breach), “Intuit Failed at ‘Know Your Customer’ Basics,” 15 March 2015, Krebs On Security, <http://krebsonsecurity.com/2015/03/intuit-failed-at-know-your-customer-basics/> (last visited 15 March 2015).

⁴ Julie P. Magee, Alabama Commissioner of Revenue, “It’s Time to Adopt a Common Objective to Stop Fraudulent Tax Refunds,” 12 March 2015, <https://www.linkedin.com/pulse/its-time-adopt-common-objective-stop-fraudulent-tax-julie> (last visited 15 March 2015).

“The hackers who targeted TurboTax this year appeared to use two techniques. Some seemed to already have people’s personal information and created fake accounts to submit phony tax returns. Others figured out users’ log-ins and passwords, by trying multiple iterations, and gained wide access to their accounts.”⁵

II. Why the Anthem Breach Was So Bad

The Target retail breach affected two overlapping groups of customers. Some had their credit or debit card numbers “RAM-scraped” from the retail terminal system before the information even entered the encryption module of the firm’s computers. But the thieves also rooted around inside Target’s computers and obtained additional general customer information, including email addresses and phone numbers, for consumers with registered Target accounts. The first set of consumers would be at risk of existing account fraud; the second set would be vulnerable to phishing expeditions. Phishing is a threat, but contrast that with Anthem.

According to widespread news reports,⁶ the Anthem breach struck a mother lode of consumer data. The theft included information on up to 80 million consumers (including some non-Anthem customers in related plans) and the data points taken included the names of employers, birth dates, social security numbers, medical account numbers, phone numbers, and home and email addresses (but no medical records). Experts believe that the Anthem data will hold strong value to thieves for years (while card numbers decline rapidly in black market value).

These data points could be used to commit a variety of more serious frauds, including obtaining your tax refund, obtaining medical care in your name and also committing financial identity theft, when new accounts are opened in your name by the thief. Names of employers and work emails could be used for spear-phishing attacks on those firms’ servers. Anthem has sent its customers a general e-mail notice and posted a website, anthemfacts.com, indicating it is conducting additional “forensics,” and will notify customers by regular mail if they were actually breached, upon its completion.

1) Many people have not even heard of medical ID theft. As the World Privacy Forum explains:

“Medical identity theft occurs when someone uses a person’s name and sometimes other parts of their identity — such as insurance information — without the person’s knowledge or consent to obtain medical services or goods, or uses the person’s identity information to make false claims for medical services or goods. Medical identity theft frequently results in erroneous entries being put into existing medical records, and can involve the creation of fictitious medical records in the victim’s name. Medical identity theft is a crime that can cause great harm to its victims. Yet

⁵ Jonnelle Marte and Craig Timberg, “Who’s to blame when fraudsters use TurboTax to steal refunds?” 4 March 2015, The Washington Post, <http://www.washingtonpost.com/news/get-there/wp/2015/03/04/unprecedented-surge-in-online-tax-scams-raises-questions-about-turbotax/> (last visited 15 March 2015).

⁶ Chad Terhune, “U.S., states probe massive data breach at health insurer Anthem,” 6 Feb 2015, Los Angeles Times, <http://www.latimes.com/business/la-fi-anthem-hack-20150207-story.html> (last visited 3 March 2015)

despite the profound risk it carries, it is the least studied and most poorly documented of the cluster of identity theft crimes. It is also the most difficult to fix after the fact, because victims have limited rights and recourses. Medical identity theft typically leaves a trail of falsified information in medical records that can plague victims' medical and financial lives for years.”⁷

2) What Can Potential Anthem Breach Victims Do? Anthem is providing a free credit monitoring service to its customers. While we and other consumer groups do not recommend taking credit monitoring if you are a victim solely of a card number breach that could result in existing account fraud, because it doesn't do any good in that circumstance and promotes a false sense of hope, we have no real objection to accepting it in this instance. Certainly, however, never pay for it.⁸ We recommend that consumers who even suspect they are identity theft victims add a 90-day, renewable initial fraud alert to their credit reports (which also entitles you to an additional free credit report).⁹ Watch your health and medical records statements carefully for at least two years to avoid medical identity theft. Take advantage of additional tips from World Privacy Forum.¹⁰

3) Next, Place a Security Freeze: Better yet, we encourage victims of the Anthem breach to place a security freeze on each of their credit reports. Indeed, any consumer who wants to proactively prevent misuse of her credit should consider a freeze. Over ten years ago U.S. PIRG, along with Consumers Union, drafted a model state security freeze law, and with the help of AARP and others, it rapidly became law in 47 states. At that point, even the generally recalcitrant credit bureaus finally capitulated and agreed to provide freezes in all jurisdictions. A security freeze prevents "new" credit from being issued in your name but allows your existing creditors to look at your report. It is the only way to prevent financial identity theft, since new creditors who cannot see credit scores or reports will not open new accounts. A freeze requires more work by you; if you want to apply for a car loan, new credit card or a home re-fi, you'll need to temporarily "lift" the freeze (you can do this on a selective or general creditor basis). A typical freeze costs \$10 (\$30 for 3) and \$5-10 each time it is temporarily lifted. A few states

⁷ World Privacy Forum, "Medical Identity Theft" page, <http://www.worldprivacyforum.org/category/med-id-theft/> (last visited 15 March 2015). The page also lists a blog dated 6 Feb 2015, "Medical ID Theft a Threat for Anthem Breach Victims, Key Tips" <http://www.worldprivacyforum.org/2015/02/medical-id-theft-a-threat-for-anthem-breach-victims-key-tips/> (last visited 15 March 2015).

⁸ However, credit monitoring firms often insist, in their terms of service, that a consumer agree that any issues be resolved through pre-dispute, or forced, arbitration. We support action by the Consumer Financial Protection Bureau or legislation to ban pre-dispute arbitration in any consumer contract, but it is especially onerous when the consumer needs the service offered because some company allowed her information to be stolen. Any federal breach legislation should ban arbitration clauses in any services offered by a breached entity or its vendors.

⁹ If you know you are an identity theft victim and file a police report or FTC affidavit demonstrating this, you can request a permanent fraud alert. More at <http://www.consumer.ftc.gov/features/feature-0014-identity-theft> (last visited 2 March 2015).

¹⁰ World Privacy Forum, "Medical ID Theft a Threat for Anthem Breach Victims, Key Tips," 6 February 2015, <http://www.worldprivacyforum.org/2015/02/medical-id-theft-a-threat-for-anthem-breach-victims-key-tips/> (last visited 15 March 2015).

offer free security freezes for identity theft victims or senior citizens.¹¹ Free security freezes for all consumers would be a logical enhancement for policymakers to consider to the federal, or state, Fair Credit Reporting Acts. While freezes are not yet free, they are much less expensive than paid credit monitoring and infinitely more effective.

III. What Steps Should Congress Take?

Congress should move carefully on data security. There is potential to benefit consumers but there is potential to make things worse.

1) Don't Override the States with A Weak Data Breach Notification Law, Especially with Broad Data Security Law Preemption: Congress should carefully weigh its response to the increase in breaches. We believe that federal breach notification legislation is unnecessary (because all firms need to do is comply with the strongest state law) and that such legislation, if it were to preempt stronger state action on data security or privacy protection, would be unwise. Most of the breach bills I have reviewed are weaker than state laws and include Trojan Horse preemption provisions eliminating not only state breach laws, but all future state actions to protect data security or privacy. That's the wrong response. Many federal proposals are also weak because they contain a "harm trigger" that allows the firm that lost your information to decide whether to tell you. Decision-making for whether to require breach notification should not be placed in the hands of a sloppy breached entity.

2) Consider Upgrades to Card Protections: Increasing consumer protections under the Electronic Funds Transfer Act (EFTA), which applies to debit cards, to the gold standard levels of the Truth in Lending Act, which applies to credit cards, should be considered. In some circumstances, consumers who lose a debit card are liable for all the money in their accounts (although they are generally well-protected if only the card data, but not the device, are taken.) Facing higher liability may "focus the mind" of the banks on improving security. Further, with new card (pre-paid cards) and device (smart phone and other technologies) being developed, it makes sense to ensure that all consumer payment systems are equally protected.

3) Rein in Credit Monitoring Advertising: Congress should also investigate the deceptive marketing of subscription-based credit monitoring, ID theft insurance, debt cancellation and other add-on products, which are over-priced and often provide a false sense of security. Credit monitoring services won't stop or warn of fraud on existing accounts. The product from Experian that was provided by Target (protectmyid) won't stop identity theft, it will simply notify you after the fact of changes to your Experian credit report (but not to your Trans Union or Equifax reports, which may include different account information). Positively, that offered product terminated after one year, rather than auto-renewing for a monthly fee (when similar products were offered after some previous breaches, the over-priced, under-performing credit

¹¹ Learn more about security freezes from Consumers Union here.

<http://consumersunion.org/research/consumers-unions-guide-to-security-freeze-protection/>

monitoring products were sometimes set to auto-renew for a fee). The products unwisely provide consumers at risk of existing account fraud a false sense of security.¹²

4) Don't Place All Blame on Merchants for Payment Card Breaches: Despite my reservations about Target's and other breached merchants') delayed and drawn out notifications to customers about their breaches and their provision of often inadequate credit monitoring product, I don't believe that Target or other merchants deserve all of the blame for the data breaches that occur on their watch.

5) The card networks are also largely at fault. They have continued to use an obsolete 1970s magnetic stripe technology well into the 21st century. When the technology was solely tied to credit cards, where consumers enjoy strong fraud rights and other consumer protections by law, this may have been barely tolerable. But when the big banks and credit card networks asked consumers to expose their own bank accounts to the unsafe signature-based payment system, by piggybacking once safer PIN-only debit cards onto the signature-based system, the omission became unacceptable. The vaunted "zero-liability" promises of the card networks and issuing banks are by contract, not law. Of course, the additional problem any debit card fraud victim faces is that she is missing money from her own account while the bank conducts an allowable reinvestigation for ten days or more, even if the bank eventually lives up to its promise.¹³

Further, the card networks' failure to upgrade, let alone enforce, their PCI or security standards, despite the massive revenue stream provided by consumers and merchants through swipe, or interchange, fees, is yet another problem caused, not by the merchants, but by the banks and card networks.

Further, the Federal Reserve Board's rule interpreting the Durbin amendment limiting swipe fees on the debit cards of the biggest banks also provides for additional fraud revenue to the banks in several ways. Even though banks and card networks routinely pass along virtually all costs of fraud to merchants in the form of chargebacks, the Fed rule interpreting the Durbin amendment allows for much more revenue. In many ways, the merchants are as much victims of the banks' unsecure systems as consumers are.¹⁴

¹² Even worse, consumers who accept the monitoring product, protectmyid from the credit bureau Experian, must accept a boilerplate forced arbitration clause that restricts their ability to sue Experian. See <http://www.protectmyid.com/terms/> And under current U.S. Supreme Court jurisprudence, that clause's outrageous ban on joining a class action is also permissible.

¹³ Compare some of the Truth In Lending Act's robust credit card protections by law to the Electronic Funds Transfer Act's weak debit card consumer rights at this FDIC website: http://www.fdic.gov/consumers/consumer/news/cnfall09/debit_vs_credit.html

¹⁴ In October 2015, changes to the PCI liability system take effect that require either the merchant or the creditor, whichever one has not upgraded, to have greater contractual liability. See, for example, <http://www.businesswire.com/news/home/20150212005260/en/U.S.-POS-Terminals-EMV-Chip-Enabled-Year-End-2015#> (last visited 15 March 2015).

IV. Detailed Recommendations:

1) Congress should not enact any federal breach law that preempts state breach laws or, especially, includes Trojan Horse preemption of other state data security rights: We make this point above. But here is more detail. 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.

From 2004-today, 46 states enacted security breach notification laws and 49 states or territories enacted security freeze laws. Many of these laws were based on the CLEAN Credit and Identity Theft Protection Model State Law developed by Consumers Union and U.S. PIRG.

A security freeze, not credit monitoring, is the best way to prevent identity theft. If a consumer places a security freeze on her credit reports, a criminal can apply for credit in her name, but the new potential creditor cannot access your "frozen" credit report and will reject the application. The freeze is not for everyone, since you must unfreeze your report on a specific or general basis whenever you re-enter the credit marketplace, but it is only way to protect your credit report from unauthorized access. See this Consumers Union page for a list of security freeze rights.

The other problem with enacting a preemptive federal breach notification law is that industry lobbyists will seek language that not only preempts breach notification laws but also prevents states from enacting any future data security laws, despite the laudable 2003 FACT Act example above. This is the Trojan Horse problem. A small federal gain should not result in a big rollback of state authority.

Simply as an example, S. 1927 (Carper) in the last Congress included sweeping preemption language that is unacceptable to consumer and privacy groups and likely also to most state attorneys general:

SEC. 7. RELATION TO STATE LAW. No requirement or prohibition may be imposed under the laws of any State with respect to the responsibilities of any person to—

- (1) protect the security of information relating to consumers that is maintained or communicated by, or on behalf of, the person;
- (2) safeguard information relating to consumers from potential misuse;
- (3) investigate or provide notice of the unauthorized access to information relating to consumers, or the potential misuse of the information, for fraudulent, illegal, or other purposes; or
- (4) mitigate any loss or harm resulting from the unauthorized access or misuse of information relating to consumers.

Other bills before the Congress have included similar, if not even more sweeping, abuses of our federal system. Such broad preemption will prevent states from acting 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.

2) Congress should improve debit/ATM card consumer rights and provide consumers with strong fraud rights not matter what card or new device they use in the payment system: Up until now, both banks and merchants have looked at fraud and identity theft as a modest cost of doing business and have not protected the payment system well enough. They have failed to look seriously at harms to their customers from fraud and identity theft – including not just monetary losses and the hassles of restoring their good names, but also the emotional harm that they must face as they wonder whether future credit applications will be rejected due to the fraudulent accounts.

Currently, debit card fraud victims are reimbursed at “zero liability” only by promise. The EFTA’s fraud standard actually provides for 3-tiers of consumer fraud losses. Consumers lose up to \$50 if they notify the bank within two days of learning of the fraud, up to \$500 if they notify the bank within 60 days and up to their entire loss, including from any linked accounts, if they notify the bank after 60 days. **However, if the physical debit card itself is not lost or stolen, consumers are not liable for any fraud charges if they report them within 60 days of their bank statement.**

This shared risk fraud standard under the EFTA, which governs debit cards, appears to be vestigial, or left over from the days when debit cards could only be used with a PIN. Since banks encourage consumers to use debit cards, placing their bank accounts at risk, on the unsafe signature debit platform, this fraud standard should be changed. Congress should also provide debit and prepaid card customers with the stronger billing dispute rights and rights to dispute payment for products that do not arrive or do not work as promised that credit card users enjoy (through the Fair Credit Billing Act, a part of the Truth In Lending Act).¹⁵

Debit/ATM card customers already face the aforementioned cash flow and bounced check problems while banks investigate fraud under the Electronic Funds Transfer Act. Reducing their possible liability by law, not simply by promise, won’t solve this particular problem, but it will force banks to work harder to avoid fraud. If they face greater liability to their customers and accountholders, they will be more likely to develop better security. Further, this review by policymakers should also ensure that improvements in consumer protection extend to all new forms of payment, including prepaid cards, smart phones and emerging technologies.

¹⁵ For a detailed discussion of these problems and recommended solutions, see Hillebrand, Gail (2008) "Before the Grand Rethinking: Five Things to Do Today with Payments Law and Ten Principles to Guide New Payments Products and New Payments Law," Chicago-Kent Law Review: Vol. 83, Iss. 2, Article 12, available at <http://scholarship.kentlaw.iit.edu/cklawreview/vol83/iss2/12>

3) Congress should not endorse a specific technology, such as EMV (parent technology of Chip and PIN and Chip and Signature). If Congress takes steps to encourage use of higher standards, its actions should be technology-neutral and apply equally to all players. Chip and PIN and Chip and signature are variants of the EMV technology standard commonly in use in Europe. The current slow U.S. rollout of Chip cards will generally provide less-secure Chip and Signature cards rather than the more-secure Chip and PIN cards. Why not go to the higher Chip and PIN authentication standard immediately and skip past Chip and Signature? Further, in his October executive order on payment card security, the President announced that all new government-issued cards would be Chip and PIN, not merely Chip and Signature.¹⁶

Of course, Congress should not embrace a specific technology. Instead, it should take steps to encourage all users to use the highest possible, best available technology-neutral performance standard. Congress should also take steps to ensure that additional technological improvements and security innovations are not blocked by actions or rules of the existing players or standards bodies.

If Congress does choose to impose higher standards, it must impose them equally on all players. For example, current legislative proposals may unwisely impose softer regimes on financial institutions already subject to the weaker Gramm-Leach-Bliley rules than to merchants and other non-financial institutions. Congress should also look at the weak requirements of the Health Insurance Portability and Accountability Act (HIPAA), which does not even require encryption.

Further, as most observers are aware, Chip technology will only prevent the use of cloned cards in card-present (Point-of-Sale) transactions. It is an improvement over obsolete magnetic stripe technology in that regard, yet it will have no impact on online transactions, where fraud volume is much greater already than in point-of-sale transactions. Experiments, such as with “virtual card numbers” for one-time use, are being carried out online. It would be worthwhile for the committee to inquire of the industry and the regulators how well those experiments are proceeding and whether requiring the use of virtual card numbers in all online debit and credit transactions should be considered a best practice.

Further, had Chip and PIN (or Chip and Signature) been in use, it would not have stopped most retail breaches, such as the Target breach, since card information was “RAM-scraped” from the Target system’s internal RAM memory, after the cards had already been used but before data were encrypted.

Technologies such as Apple-Pay offer additional promise, but are often not as good as they are trumped up to be. Recently, “low-tech” thieves figured out that they could use forged or stolen or

¹⁶ The White House, “Executive Order --Improving the Security of Consumer Financial Transactions,” 17 October 2014, available at <https://www.whitehouse.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions> (last visited 16 March 2015).

cloned cards on the Apple Pay system because banks were not verifying that the card entered into the phone was itself legitimate.¹⁷

4) Investigate Card Security Standards Bodies and Ask the Prudential Regulators for Their Views: To ensure that improvements continue to be made in the system, the committee should also inquire into the governance and oversight of the development of card network security standards. Do regulators sit on the PCI board? As I understand it, merchants do not; they are only allowed to sit on what may be a meaningless “advisory” board. Further, do regulators have any mandatory oversight function over standards body rules? Are standards bodies open or closed? Does a closed standards body serve the public interest?

5) Congress should not enact any new legislation sought by some banks and credit unions to impose their costs of replacement cards on the merchants by law: Breached merchants should pay their share but breaches are not entirely a merchant’s fault when the merchant has been forced to build an ever-higher wall to protect a dangerous, defective device, the magnetic stripe card. Disputes over costs of replacement cards should be handled by contracts and agreements between the players. How could you possibly draft a bill to address all the possible shared liabilities? Further, going forward, amendments to the PCI rules will impose greater liability on firms that have not adopted higher standards. For example, if a merchant’s technology does not accept CHIP cards, it would face greater liability. If a merchant does accept CHIP cards, but the bank has not replaced its magnetic stripe cards, the bank would face higher liability.

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.

Many of the data breach bills I have seen specifically state that no private right of action is created. Such clauses should be eliminated and it should also be made clear that the bills have no effect on any of the 17 state law private rights of action. 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) No Federal Breach Law Should Include Any “Harm Trigger” Before Notice Is Required: The better state breach laws, including California and Illinois among others, require breach notification if information is presumed to have been “acquired.” The weakest laws allow the company that failed to protect the consumer’s information in the first place to decide whether to tell them, based on its estimate of the likelihood of identity theft or other harm. We call this a

¹⁷ Robin Sidel and Daisuke Wakabayashi, “Apple Pay Stung by Low-Tech Fraudsters,” 5 March 2015, Wall Street Journal, <http://www.wsj.com/articles/apple-pay-stung-by-low-tech-fraudsters-1425603036> (last visited 15 March 2015).

“harm trigger.” The worst harm triggers also define harm quite narrowly, when privacy advocates are well aware of the kinds of additional problems victimized consumers face.

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.

8) Any Bill That Purports to Protect Personally Identifiable Information Should Broadly Define Personal Information: Some federal data breach proposals define “Personally Identifiable Information” (PII) too narrowly. For example, under Florida’s data security and breach notification law, the definition of personal information includes an email address and password combination.¹⁸ Florida’s law also protects a wide range of information about physical and mental health, medical history, and insurance, as do the state laws of California, Missouri, New Hampshire, North Dakota, Texas, and Virginia.¹⁹ Many federal bills do not include protection for this sort of information in the event of a breach. Some state laws and proposed state laws may also include geolocation or marketing information in their definition of PII. Not all federal proposals consider these data points in their narrow definitions of protected PII. As a news release explained Illinois Attorney General Lisa Madigan’s recent testimony to the U.S. Senate:

“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.²⁰”

¹⁸ See http://www.leg.state.fl.us/statutes/index.cfm?App_mode=Display_Statute&Search_String=&URL=0500-0599/0501/Sections/0501.171.html

¹⁹ See, for example,

http://www.bakerlaw.com/files/Uploads/Documents/Data%20Breach%20documents/State_Data_Breach_Statute_Form.pdf

²⁰ 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 (last visited 15 March 2015). General

9) Congress should further investigate marketing of overpriced credit monitoring and identity theft subscription products: In 2005 and then again in 2007 the FTC imposed fines on the credit bureau Experian for deceptive marketing of its various credit monitoring products, which are often sold as add-ons to credit cards and bank accounts. Banks receive massive commissions for selling them to their own customers. While it is likely that recent CFPB enforcement orders²¹ against several large credit card companies for deceptive sale of the add-on products – resulting in refunds to date of over \$1.5 billion to aggrieved consumers -- may cause 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.

In addition to profits from credit monitoring, banks and other firms reap massive revenues from ID Theft insurance, sometimes sold in the same package and sometimes sold separately. Lifelock, a major 3rd party company in the identity protection space, was fined in 2010 for deceptive marketing, in an action brought by the FTC and 35 states.²² Prices for these products from credit bureaus, Lifelock and others range up to \$19.99/month. Companies that don't protect our information as the law requires add insult to injury by pitching us these over-priced monitoring and insurance products. The committee should call in the companies that provide ID theft insurance and force the industry to open its books and show what percentage of premiums are paid out to beneficiaries. It is probable that the loss ratio on these products is so low as to be meaningless, meaning profits are sky-high.

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.

Madigan's testimony before the U.S. Senate Commerce Committee on that date is available at <http://1.usa.gov/1tGft5m> (last visited 15 March 2015).

²¹ We discuss some of the CFPB add-on cases here <http://www.uspirg.org/blogs/eds-blog/usp/cfpb-gets-results-consumersand-taxpayers-too> (last visited 15 March 2015).

²² FTC, "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, <https://www.ftc.gov/news-events/press-releases/2010/03/lifelock-will-pay-12-million-settle-charges-ftc-35-states> (last visited 15 March 2015).

Although federal authority against unfair monitoring marketing was improved in the 2009 Credit CARD Act,²³ the committee should also ask the regulators whether any additional changes are needed.

10) Congress Should Review Title V of the Gramm-Leach-Bliley Act and its Data Security

Requirements: The 1999 Gramm-Leach-Bliley Act imposed modest data security responsibilities on regulated financial institutions, a broader category than simply banks. The requirements include breach notification, but only in certain risk-determined circumstances.²⁴ The committee should ask the regulators for information on their enforcement of these requirements and should determine whether additional legislation is needed, especially in light of the recent JP Morgan Chase breach. The committee should also recognize, as noted above, that mere compliance with weak GLBA guidance should not constitute constructive compliance with any additional security duties imposed on other players in the card network system as that could lead to a system where those other non-financial-institution players are treated unfairly.

11) Congress Must Not Weaken the Communication Act’s Broad Privacy Protections:

Leading consumer and privacy groups are also concerned that the powerful phone and cable companies seek to convince Congress to serve them, not the public interest, by using data breach legislation as an opportunity to move yet another Trojan Horse provision. They seek to weaken existing privacy protections for telephone metadata under Customer Proprietary Network Information (CPNI) regulations. They seek to rescind important provisions of the Communications Act that protect the personal information of telecommunications, cable, and satellite customers. As my privacy advocacy colleague Laura Moy of the New America Foundation explained to the Energy and Commerce Committee today:²⁵

“The move against CPNI could not come at a worse time, because the Federal Communications Commission has just voted to reclassify broadband Internet access as a telecommunications service under Title II of the Communications Act, enabling it to apply the CPNI provision of the Communications Act to broadband. Applied to broadband, the CPNI provisions will require Internet service providers to protect information about use of the service that, as gatekeepers, they are in a unique position to collect: information such as what sites an Internet user visits and how often, what apps she uses, and what wireless devices she owns.”

²³ The Credit Card Accountability, Responsibility and Disclosure (CARD) Act of 2009, Public Law 111-24. See Section 205.

²⁴ See the Federal Financial Institutions Examination Council’s “Final Guidance on Response Programs: Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice,” 2005, available at <http://www.fdic.gov/news/news/financial/2005/fil2705.html>

²⁵ Hearing on a Discussion Draft of HR ____, Data Security and Breach Notification Act of 2015, Subcommittee on Commerce, Manufacturing, and Trade, U.S. House of Representatives, 18 March 2015, available at <http://energycommerce.house.gov/hearing/discussion-draft-hr-data-security-and-breach-notification-act-2015> (last visited 16 March 2016).

V. 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 poses threats as a business model itself.

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.

The 1970 Fair Credit Reporting Act, for all its flaws our strongest privacy law, is largely based on the Code of Fair Information Practices.²⁶ Further, it limits the use of financial information for secondary purposes. The only marketing purposes allowed are credit and insurance marketing and then only after the law gives consumers the right to opt-out of those limited allowed uses.

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.²⁷ The Federal Trade Commission has called for additional legislation to rein in the practices of largely unregulated data brokers. Here is a brief excerpt from the FTC's release accompanying its 2014 report:²⁸

²⁶ Bob Gellman, "Fair Information Practices: A Basic History", 11 February 2015, available at <http://bobgellman.com/rg-docs/rg-FIPShistory.pdf> (last visited 15 March 2015) Advocates consider the 1980 OECD version to be the best application of the FIPs.

²⁷ See the FTC's March 2012 report, "Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers," available at <http://www.ftc.gov/news-events/press-releases/2012/03/ftc-issues-final-commission-report-protecting-consumer-privacy>. Also 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/selling-consumers-not-lists/> (last visited 15 March 2015).

²⁸ Federal Trade Commission, "FTC Recommends Congress Require the Data Broker Industry to be More Transparent and Give Consumers Greater Control Over Their Personal Information," 27 May 2014, available at

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. [...] Among the report's findings:

-- Data brokers collect consumer data from extensive online and offline sources, largely without consumers' knowledge, ranging from consumer purchase data, social media activity, warranty registrations, magazine subscriptions, religious and political affiliations, and other details of consumers' everyday lives.[...]

-- 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.

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.²⁹

VI. Conclusion: Consumers Need A Real Consumer Privacy Bill of Rights

Recently, the administration proposed a Consumer Privacy Bill of Rights. The original administration blueprint, in 2012, was encouraging.³⁰ However, this month we joined many other consumer and privacy groups,³¹ and even leaders of the Federal Trade Commission,³² an

<https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more> (last visited 16 March 2015).

²⁹ This paragraph is taken from a 2014 report, 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 <http://www.uspirg.org/reports/usf/big-data-means-big-opportunities-and-big-challenges> (last visited 16 March 2015).

³⁰ The White House, "We Can't Wait: Obama Administration Unveils Blueprint for a "Privacy Bill of Rights" to Protect Consumers Online," 12 February 2012, available at <https://www.whitehouse.gov/the-press-office/2012/02/23/we-can-t-wait-obama-administration-unveils-blueprint-privacy-bill-rights> (last visited 15 March 2015).

³¹ Letter from Consumer and Privacy Groups to Congress Opposing Draft Administration Consumer Privacy Bill of Rights, 3 March 2015, available at <http://www.consumerwatchdog.org/resources/ltrobamagroups030315.pdf> (last visited 15 March 2015).

³² FTC Commissioner Julie Brill is quoted by Rich Lord in the Pittsburgh Post-Gazette, "FTC Commissioner Brill, privacy advocate, 'disappointed' with White House proposal," 8 March 2015, available at <http://www.post-gazette.com/news/nation/2015/03/08/FTC-Commissioner-Brill-privacy-advocate-disappointed-with-White-House-proposal/stories/201503080132> (last visited 15 March 2015). Chairwoman Edith Ramirez also made public criticisms.

independent agency, in criticizing the approach taken in the draft, which appears to allow all existing marketplace practices, no matter how abusive or intrusive, to continue.

Congress has 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.

Any bill should adequately define what constitutes sensitive information, and provide consumers with meaningful choices about this 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.

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.

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



January 2015

Biography of Edmund Mierzwinski, U.S. PIRG Consumer Program Director and Senior Fellow

Ed Mierzwinski has worked in the Washington, DC-based federal lobbying office of the Federation of State Public Interest Research Groups (U.S. PIRG) since 1989. He often lectures or testifies before Congress, state legislatures and agencies on a wide range of consumer issues, from credit card rates and privacy to product safety and airline passenger rights. He has published reports on numerous consumer issues, including Big Data's impact on financial opportunity, the CFPB Public Consumer Complaint Database, internet privacy, identity theft and credit reporting mistakes. He is co-author of a Model State Data Breach, Security Freeze and Identity Theft Law available on SSRN. He has had recent articles in the *American Prospect*, the *Journal of Consumer Affairs* and the *Suffolk University Law Review*.

He is a 2003 recipient of Privacy International's "Brandeis Award" for privacy protection efforts and a 2006 recipient of the Consumer Federation of America's "Esther Peterson Consumer Service Award." For the last 5 years, "The Hill" newspaper has selected him as a "Top Lobbyist" awardee and, in 2011, *Bloomberg Businessweek* selected him as one of "15 Power Brokers: Regulators, lawmakers and lobbyists shaping the torrent of regulations."

In August 2012, he was re-elected to a second 3-year term on the board of directors of Consumer Reports (formerly Consumers Union), the world's largest consumer product testing and advocacy organization. He chairs the Americans for Financial Reform (AFR) Consumer Financial Protection Bureau Task Force. He is a founding and current member of the Steering Committee of the Transatlantic Consumer Dialogue (tacd.org). He is on the board of directors of Flyersrights.org. He is a former member of the Federal Reserve Board's Consumer Advisory Council. He is a graduate of the University of Connecticut (BA, MS) and previously was Executive Director of the Connecticut PIRG.

Ed Mierzwinski, edm@pirg.org or direct line 202-461-3821

Ed's blog, <http://www.uspirg.org/consumer-blog> Twitter @edmpirg

Committee on Oversight and Government Reform
Witness Disclosure Requirement – “Truth in Testimony”
Required by House Rule XI, Clause 2(g)(5)

Name: Edmund Mierzwinski, U.S. PIRG

1. Please list any federal grants or contracts (including subgrants or subcontracts) you have received since October 1, 2012. Include the source and amount of each grant or contract.

NONE

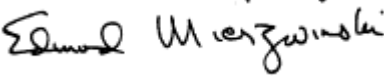
2. Please list any entity you are testifying on behalf of and briefly describe your relationship with these entities.

I am fulltime staff for U.S. Public Interest Research Group. I serve as Consumer Program Director. I have worked there for 25 years. U.S. PIRG is a non-profit, non-partisan organization.

3. Please list any federal grants or contracts (including subgrants or subcontracts) received since October 1, 2012, by the entity(ies) you listed above. Include the source and amount of each grant or contract.

NONE

I certify that the above information is true and correct.

Signature: 
Date:

16 March 2015
