Testimony of Edmund Mierzwinski

U.S. PIRG Consumer Program Director

at a hearing on

"Data Security: Examining Efforts To Protect Americans' Financial Information"

Before the House Financial Services Committee

Subcommittee on Financial Institutions and Consumer Credit

Honorable Shelley Moore Capito, Chair

5 March 2014

Testimony of Edmund Mierzwinski, U.S. PIRG Consumer Program Director at a hearing on "Data Security: Examining Efforts To Protect Americans' Financial Information," Before the House Financial Services Subcommittee on Financial Institutions and Consumer Credit, 5 March 2014

Chair Capito, Representative Meeks, members of the committee, I appreciate the opportunity to testify before you on the important matter of consumer data security. Since 1989, I have worked on data privacy issues, among other financial system 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, fully 664,065,960 records have been breached in a total of 4,188 separate data breaches.[1] According to the Clearinghouse, the most recently reported breach is that Sears announced last Friday that the Secret Service is investigating Sears Holdings Corporation as a target of a similar security breach to the ones that hit Target and Neiman Marcus at the end of 2013. That recent exploit against Target Stores, depending on how it is measured, is among the largest ever.

Target, Neiman and other merchants should be held accountable for their failure to comply with applicable security standards but that does not mean they are 100% responsible for breaches. Merchants, and their customers, have been forced by the card monopolies to use an unsafe payment card system that relies on obsolete magnetic stripe technology, buttressed by a constantly changing set of so-called PCI standards to compensate for the inherent flaws of the underlying, ancient tech. When the mag stripe technology was used only for safer credit cards, this may have been acceptable, but since the banks and card networks have also aggressively promoted the use of debit cards on the unsafe signature (not safer PIN) based platform, consumer bank accounts have also been placed at risk.

Congress should carefully weigh its response to recent breaches. 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 the first step. Facing higher liability may "focus the mind" of the banks on improving security. Second, Congress should not preempt the strongest state breach notification laws, especially with a federal breach law that may include a Trojan Horse preemption provision eliminating not only state breach laws, but all future state actions to protect privacy. That's the wrong response as we discuss below. Finally, Congress should also investigate the deceptive marketing of subscription-based credit monitoring and ID theft insurance products, which are over-priced and provide a false sense of security. In this case, although the highest risk to consumers is fraud on existing accounts, the modest credit monitoring product offered (for free) to Target customers will at best

[1] See "Chronology of Data Breaches," Privacy Rights Clearinghouse, last visited 4 March 2014 https://www.privacyrights.org/data-breach.

tell you that you have already become an identity theft victim. We make additional recommendations in the testimony below and are at all times available to brief committee staff or members.

The Target Breach (as an example):

The card information acquired in the first 40 million breached accounts that Target reported placed those debit/ATM or credit card customers at **risk of fraud on their existing accounts**. Because the scope of the records acquired in that RAM-scraping incident included not only the card number but also the expiration date, 3-digit security code (from the back of the card) and the (encrypted but probably hackable) PIN number or password, these numbers became very valuable on the underground market, as the Secret Service and Homeland Security have probably already explained. Subsequent reports on the Target breach indicate that the point of entry was a vendor's computer link for invoicing, and that that link allowed access to virtually all internal data systems, including those that contained the customer information.

In addition to RAM-scraping from the its store point-of-sale terminal systems, Target later admitted that additional information – including telephone numbers and email addresses – for up to a total of 70-110 million consumer records (some may have been the same consumers) held in a Customer Relations Management (CRM) database was also obtained, which places those customers **at the risk of new account identity theft.** Criminals will seek to obtain additional information, such as a consumer's Social Security Number, which would enable them to submit false applications for credit in your name.

When bad guys obtain emails and phone numbers, they make phishing attacks to obtain more information: While the email addresses and phone numbers are not enough information to commit identity theft, it is enough information to conduct such "phishing attacks" designed to collect additional information, including Social Security Numbers and encrypted passwords, from consumers.

They do this either through placing dangerous links in emails or using various "social engineering" techniques to trick you into providing more information. A phishing email will appear to be from your bank. But if you click on any links, either a virus explodes on your computer to collect any personal information stored on it, or you are redirected to a site that will allow them to obtain the information they need. Or, if they call you, they use the information that they have as a validation that they are from the bank, to trick you into providing the information that they need.

The additional information the bad guys seek, then, would either allow them direct access to your account (through the PIN) 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 and Social Security Number. They hope to trick you into giving it up.

However, I believe the greater risk in this case is fraud on existing accounts, not identity theft. That is why so many banks re-issued debit and credit cards, or both, following the incident. But disappointingly, Target's main response to consumers – offering a free credit monitoring service – won't stop or warn of fraud on existing accounts. That provides consumers a false sense of security.[2]

It actually won't even 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, the offered product terminates 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 monitoring products were sometimes set to auto-renew for a fee).

Despite my reservations about Target's delayed and drawn out notifications to customers about the breach,[3] and its provision of the 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.

The card networks are 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 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.[4] Further, the contractual promises I have seen contain asterisks and exceptions, such as for a consumer who files more than one dispute in a year.

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 outrage by the banks and card networks.

---

[2] 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.

[3] I understand that some state Attorneys General are investigating whether adequate notification was made under their breach laws.

[4] 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

Incredibly, 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. So, not only are banks and card networks compensated with general revenue from the ever-increasing swipe fees, but the Fed allows them numerous additional specific bites of the apple for fraud-related fees.

To be sure, Target should be held accountable if it turns out, as has been reported, that it was not in compliance with the latest and highest level of security standards throughout its system. But understand that that system was inadequate at best because, like acting as any monopolists would, the card duopoly refused to make adequate technological improvements to its system, preferring to extract excess rents for as long as possible. For that reason, I cannot endorse any reform that makes Target, or other merchants, the only ones at blame. In many ways, the merchants are as much victims of the banks' unsecure systems as consumers are.

Recommendations:

1) Congress should improve debit/ATM card consumer rights and make all plastic equal:

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.

As a first step, Congress should institute the same fraud cap, $50, on debit/ATM cards as exists on credit cards. (Or, even eliminate the cap of $50 in all cases, since it is never imposed.) 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).[5]

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.

2) Congress should not endorse a specific technology, such as EMV (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 pending U.S. rollout of chip cards will allow use of the 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? As I understand the rollout schedule, there is still time to make this improvement. Ask the bank and card network witnesses today for an explanation.

This example demonstrates why Congress should not embrace a specific technology. Instead, it should take steps to encourage all users to use the highest possible existing 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.

If Congress does choose to impose higher standards, then it must impose them equally on all players. For example, current legislative proposals may unwisely impose softer regimes on financial institutions subject to the weaker Gramm-Leach-Bliley rules than to merchants and other non-financial institutions.

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.

[5] 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

Further, as I understand it, had Chip and PIN (or Chip and Signature) been in use, it would not have stopped the Target breach, since unencrypted information was collected from the Target system's internal RAM memory, after the cards had already been used.

3) 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?

Recently, the networks have been in to see the Federal Reserve Board ostensibly to talk about interchange (swipe) fees. Since the Fed is not a witness today, the committee should ask the Fed and other prudential regulators about these matters at in letters or at any future hearings about these matters. In particular, ask the Fed to testify as to the purposes and discussions at these meetings held with the banks and card networks. Its summary of one of these meetings indicates that the issue was EMV (CHIP card technology) rollout:

> Summary (Meeting Between Federal Reserve Board Staff and Representatives of Visa, January 8, 2014) : Representatives of Visa met with Federal Reserve Board staff to discuss their observations of market developments related to the deployment of EMV (i.e., chip-based) debit cards in the United States. Topics discussed included an overview of their current EMV roadmap and Visa's proposed common application for enabling multiple networks on an EMV card while preserving merchant routing and choice.[6]

4) Congress should <u>not</u> enact any new legislation sought by the banks to impose their costs of replacement cards on the merchants:

Target should pay its share but this breach was not entirely Target's fault. The merchants are forced to use an obsolete and unsafe system designed by the banks and card networks, which, to make matters worse, don't uniformly enforce their additional often-changing security standards intended to ameliorate the flaws in the underlying platform. 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?

Of course, the Federal Reserve has already allowed compensation to banks for card replacement in circumstances where the Fed's Durbin amendment rule applies. It states:

> "Costs associated with research and development of new fraud-prevention technologies, card reissuance due to fraudulent activity, data security, card activation, and merchant blocking are all examples of costs that are incurred to detect and prevent fraudulent electronic debit transactions. Therefore, the Board has included the costs of these activities in setting the fraud prevention

[6] Available at http://www.federalreserve.gov/newsevents/rr-commpublic/pin-debit-networks-20131107.pdf

adjustment amount to the extent the issuers reported these costs in response to the survey on 2009 costs."[7]

Under the Fed's Durbin rules the amount of this compensation is as follows: banks can also get 5 basis points per transaction for fraud costs, 1.2 cents per transaction for transaction monitoring, and 1 cent per transaction for the fraud prevention adjustment. Again, this is in addition to merchants already paying chargebacks for fraud as well as PCI violation fines, plus litigation damages.

5) Congress should <u>not</u> enact any federal breach law that preempts state breach laws or, especially, preempts other state data security rights:

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.[8] 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 state 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.[9]

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 footnoted Consumers Union page for a list of security freeze rights.[10]

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.

[7] See 77 Fed. Reg. page 46264 (August 3, 2012), available at http://www.gpo.gov/fdsys/pkg/FR-2012-08-03/pdf/2012-18726.pdf.

[8] See "conduct required" language in Section 711 of the Fair and Accurate Credit Transactions Act of 2003, Public Law 108-159. Also see Hillebrand, Gail, "After the FACT Act: What States Can Still Do to Prevent Identity Theft," Consumers Union, 13 January 2004, available at http://consumersunion.org/research/after-the-fact-act-what-states-can-still-do-to-prevent-identity-theft/

[9] See http://consumersunion.org/wp-content/uploads/2013/02/model.pdf

[10] http://defendyourdollars.org/document/guide-to-security-freeze-protection

Simply as an example, S. 1927 (Carper) includes 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.

Most other bills before the Congress include similar, if not even more sweeping, abuses of our federal system, although HR 3990, "The Personal Data Privacy and Security Act of 2014," appears to have a narrower preemption scheme that may be intended to apply only to data breach notification.

At least one merchant I have spoken with told me: "Actually, Ed, it is relatively easy to comply with the different state breach laws. We haven't had a problem."

Such broad preemption will prevent states from acting as first responders to emerging privacy threats. Congress should not preempt the states. In fact, Congress should think twice about whether a federal breach law that is weaker than the best state laws is needed at all.

6) Congress Should Allow For 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 enforcement of those laws, buttressed by state and local and private enforcement.

Many of the data breach bills I have seen specifically state 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 state 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.

For example, in California not only the state Attorney General but also county District Attorneys and even city attorneys of large cities can bring unfair practices cases.

Although we currently have a diamond age of federal enforcement, with strong but fair enforcement agencies including the CFPB, OCC and FDIC, that may not always be the case. By preserving state remedies and the authority of state and local enforcers, you can better protect your constituents from the harms of fraud and identity theft.

7) Any federal breach law should not include any "harm trigger" before notice is required:

The better state breach laws, starting with California's, require breach notification if information is presumed to have been "acquired." The weaker 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.

Only an acquisition standard will serve to force data collectors to protect the financial information of their trusted customers, accountholders or, as Target calls them, "guests," well enough to avoid the costs, including to reputation, of a breach.

8) 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. Prices range up to $19.99/month. While it is likely that recent CFPB enforcement orders[11] against several large credit card companies for deceptive sale of the add-on products – resulting in recovery of approximately $800 million 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. Companies that don't protect our information as the law requires add insult to injury by pitching us 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.

[11] We discuss some of the CFPB cases here http://www.uspirg.org/news/usp/cfpb-gets-results-orders-chase-bank-repay-consumers-over-300-million-over-sale-junky-credit

Although federal authority against unfair monitoring marketing was improved in the 2009 Credit CARD Act,[12] the committee should also ask the regulators whether any additional changes are needed.

9) Review Title V of the Gramm-Leach-Bliley Act and its Data Security Requirements:

The 1999 Gramm-Leach-Bliley Act imposed data security responsibilities on regulated financial institutions, including banks. The requirements include breach notification in certain circumstances.[13] The committee should ask the regulators for information on their enforcement of its requirements and should determine whether additional legislation is needed. The committee should also recognize, as noted above, that compliance with GLBA 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.

10) Congress should investigate the over-collection of consumer information for marketing purposes. More information means more information at risk of identity theft. It also means there is a greater potential for unfair secondary marketing uses of information:

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 localized information.

Although the Fair Credit Reporting Act limits the use of financial information for marketing purposes and gives consumers the right to opt-out of the limited credit marketing uses allowed, these new Big Data uses of information may not be fully regulated by the FCRA. The development of the Internet marketing ecosystem, populated by a variety of data brokers and advertisers buying and selling consumer information without their knowledge and consent, is worthy of Congressional inquiry.[14] **Thank you for the opportunity to provide the Committee with our views. We are happy to provide additional information to Members or staff.**

---

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

[13] 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

[14] 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), also available at http://suffolklawreview.org/selling-consumers-not-lists/