Testimony of Edmund Mierzwinski

U.S. PIRG Consumer Program Director

at a hearing on

"The EMV Deadline and What it Means for Small Businesses: Part II"

Before the House Small Business Committee

Honorable Steve Chabot, Chair

21 October 2015

Testimony of Edmund Mierzwinski, U.S. PIRG Consumer Program Director at a hearing on "The EMV Deadline and What it Means for Small Businesses: Part II"," Before the House Small Business Committee, 21 October 2015

Chair Chabot, Representative Velázquez, members of the committee, I appreciate the opportunity to testify before you on the important matter of consumer data security and the implications of the 1 October 2015 EMV liability change for small businesses and their consumer customers. Since 1989, I have worked on data privacy, among other financial 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:
Chip and PIN is Safer than Chip and Signature: Since the 1970s, the U.S. credit card, and later, also debit card, markets relied on magnetic stripe verification technology. To better deter "card-present" or in-person fraud, Canada and Europe switched to much stronger Chip and PIN technology over a decade ago. The U.S. is finally transitioning to Chip cards, although most banks are expected to offer the less robust Chip and Signature, rather than Chip and PIN, cards. Chips prevent information from your card from being transferred into merchant computers and prevent your card from being cloned. PINs prove you are not an imposter. Note that neither technology will deter online fraud, only in-person (card-present) fraud.

To accelerate the belated conversion of the U.S. system at least to Chip, or EMV (Europay, Mastercard and Visa), systems, the Payment Card Industry (PCI) security standards body made a scheduled liability change on 1 October 2015. As of that date, merchants face greater fraud liability if they have not installed card readers that accept Chip cards. Banks that have not issued Chip cards retain greater liability. Gas stations have a longer implementation period.

Banks Make More Money From Signature Transactions: While the banks have a polished narrative making other explanations as to "Why Chip, not Chip and PIN?", it really comes down to one factor: Visa and Mastercard have long functioned as a cartel with market power to drive traffic to their own payment networks -- which are signature-enabled, not PIN enabled. They earn much higher merchant "swipe" or interchange fees. As merchant witnesses will explain, they already faced significant liability as well as are limited in their choices by card network rules. All consumers, including cash customers, pay more at the store and more at the pump due to these rules, which drive traffic to the higher-cost, yet riskier signature platforms, not PINs, quite simply because Visa and Mastercard profit more from transactions on those platforms. In either case, lower-income cash customers end up subsidizing more-affluent rewards card customers because merchants bake the cost of swipe fees into their prices.

We urge no preemptive federal action on data breaches: For several years Congress has considered national data breach notification legislation. Nearly every proposal I have seen, including numerous bills before this Congress, contains an onerous Trojan Horse provision. Even though most federal bills provide only extremely limited consumer protections, they broadly preempt state data security and consumer protection laws. Data breaches can result in numerous

types of harms yet the bills do not recognize all the harms. The states have already implemented data breach notice laws that are working well.

I will discuss each of these points in greater detail in the following discussion.

Discussion:

The transition to Chip cards means merchant data breaches will no longer act as such a treasure trove of account numbers and expiration dates for existing account fraud. The Chip technology prevents the transfer of the full card number and expiration date to the merchant, who will receive only a one-time transaction code. The Chip cannot be cloned, meaning counterfeit cards usable in Chip "dip" readers cannot be created from the information available after a data breach. Of course, many cards will be backward-compatible for some time (still have a magnetic stripe to be "swiped") but these will be used at fewer and fewer card readers over time, limiting their value to bad guys going forward.

However, we remain concerned that most U.S. banks and credit unions are expected to convert only to Chip cards, not fully to Chip and PIN cards, which are safer for consumers and preferred by merchants, both of whom will still face the problems of stolen Chip cards in a "Chip and Signature" world. Chips prove your card is not a clone; PINs prove you are not an imposter.

So far, we are only aware of one bank, upstate New York's First Niagara Bank, that's gone beyond Chip and Signature and is rolling out the more robust Chip and PIN.[1] Positively, President Obama ordered last year that all U.S. issued credit cards and all U.S. agency card readers be Chip-and-PIN.[2]

When debit or credit card **numbers** only are stolen, such as in a breach, consumer protections are quite strong, although debit card customers may face cash flow problems while they wait for the bank to conduct a reinvestigation and replace money in their accounts. However, when debit cards themselves are lost, debit card customers face much greater liability, much more quickly.

The December 2013 Target stores breach ultimately affected some 110 million customers and Target accountholders. The first tranche of some 40 million customers had their card numbers skimmed or "scraped" off the card reader software and made consumers vulnerable to existing account fraud, forcing numerous banks to replace cards.[3] But the Target breach was only one in a long series of breaches, and an increase in card fraud generally, that had led to the proposal for the EMV card switch.

---

[1] See Matt Glynn, " First Niagara rolling out Chip-and-PIN cards", Buffalo News, 30 September 2015 http://www.buffalonews.com/business/first-niagara-rolling-out-Chip-and-pin-cards-20150930

[2] See Fred Williams, "Obama puts federal might behind Chip-and-PIN card security Social Security, other federal payment cards to switch in 2015," http://www.creditcards.com/credit-card-news/obama-federal-backs-Chip-and-pin-1282.php

[3] After the thieves rooted around inside the Target mainframe for some time, they obtained phone numbers and email addresses for many more consumers with Target accounts. These data could then be used for social engineering or "phishing" attacks designed to obtain the additional information – Social Security Numbers and birth dates – that make it possible to commit "new account identity theft."

Target and other breached 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, had 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 stripe tech.

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 a step taken by Congress. While EFTA provides for zero liability if a consumer notifies her bank within 60 days after her debit card number, but not her card, is stolen, she still faces the stigma of bouncing checks and cash flow problems while waiting for the bank to reinstate her funds, which is a problem for consumers living from paycheck to paycheck. But if a debit card is stolen, liability by law of up to $500 begins to accrue if the bank is not notified within 2 days. After 60 days, liability could be greater than $500 and could include funds taken from linked accounts. Conversely, the Truth In Lending Act grants credit card customers very strong protections in all cases, plus, no money is ever removed from your own bank account by credit card thieves.

The card networks continued to use an obsolete 1970s magnetic stripe technology well into the 21st century because, as oligopolists, they wanted to extract greater rents from the system. When the technology was solely tied to credit cards, where consumers enjoyed 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 ATM cards onto the signature-based system after re-branding them as "debit" cards, 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. 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]

[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

[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, the card networks' failure to upgrade, let alone enforce, their PCI 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.

Merchants that accept credit and debit cards are already subject to a set of fees and a set of rules. The full "swipe fee" includes a small fee paid to the network, a small fee paid to the merchant's bank and a very large interchange fee paid to the consumer's bank. Merchants also pay third-party processing fees. A portion of the interchange fee is already allocated to fraud prevention. Merchant swipe fees (deducted from the payments they receive from banks) could range from about 1% for a "classic" debit card to 3.5% or more for an airline rewards credit card. (The fee schedules are complex and the fee often includes a flat fee plus a percentage of the cost of the transaction. Different merchant classes pay different fees.)

Rules include both the security compliance standards set by the Payment Card Industry (PCI) process that led to this liability shift as well as to additional complex network rules.[6]

Incredibly, the Federal Reserve Board's rule interpreting the Durbin amendment to the 2010 Dodd-Frank Wall Street Reform and Consumer Protection Act, which limited swipe fees on the debit cards of the biggest banks, also provided for additional fraud revenue to the banks in several ways. Even though banks and card networks have routinely passed along virtually all costs of fraud to merchants in the form of chargebacks, the Federal Reserve 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.[7]

Under the Fed's Durbin rules the amount of this additional 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, and, now, possible additional direct costs of fraud for failing to install Chip readers.

Unfortunately, without PINs, the EMV transition will not provide merchants and consumers the level of protection against fraud that they both seek.

Further, while most news discussion and bank political advertising related to the Durbin amendment focuses on bank complaints about both the reduced revenue stream and the merchants' purported failure to pass along savings, it is important to understand that other provisions of the amendment were also important. For example, the Durbin amendment makes it easier for merchants to "signal" to consumers that certain payment methods, including the use of

[6] These network rules set by Visa and Mastercard, as well as by Discover and American Express, have been the subject of a variety of public and private antitrust lawsuits over many years but are not directly the subject of this testimony.

[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.

alternative networks, cost them less and are preferred. Of course, the least-costly networks are generally PIN-based, but most consumers, thanks to banks only moving partway, will not have PIN cards.

We are only aware of one bank, upstate New York's First Niagara Bank, that's gone beyond Chip and Signature and is rolling out the more robust Chip and PIN.[8] Positively, President Obama ordered last year that all U.S. issued credit cards and all U.S. agency card readers be Chip-and-PIN.[9]

This month, the FBI offered but then immediately "walked back" a recommendation to consumers and merchants that Chip and PIN is better than Chip and Signature. As Senator Durbin asked in a letter to FBI director Comey last week:

> "The revisions to the FBI advisory raise significant questions about whether current EMV security technology is adequately protecting consumers and whether the FBI is taking appropriate steps to warn against and deter payment card fraud involving lost or stolen cards," said Durbin. "Did representatives of the American Bankers Association contact the FBI between the issuance of the October 8 advisory and the release of the revised advisory? If so, did the American Bankers Association request that the advisory's recommendations for consumers and merchants to use PINs be removed?[10]"

The committee should join Senator Durbin in asking Director Comey these questions.

We believe that if Congress acts in the payment card security, it should take steps, as the President did, 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. In general, this means proposing or encouraging a technology-neutral performance standard.

If Congress does choose to impose higher standards, then it must alsoimpose 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

[8] See Matt Glynn, " First Niagara rolling out Chip-and-PIN cards", Buffalo News, 30 September 2015 http://www.buffalonews.com/business/first-niagara-rolling-out-Chip-and-pin-cards-20150930

[9] See Fred Williams, "Obama puts federal might behind Chip-and-PIN card security Social Security, other federal payment cards to switch in 2015," http://www.creditcards.com/credit-card-news/obama-federal-backs-Chip-and-pin-1282.php

[10] See "Durbin Calls for FBI to Explain Walkback of Consumer Protection Advisory Regarding Security Features on Credit and Debit Cards," 15 October 2015, http://www.durbin.senate.gov/newsroom/press-releases/durbin-calls-for-fbi-to-explain-walkback-of-consumer-protection-advisory-regarding-security-features-on-credit-and-debit-cards

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.

Congress should <u>not</u> enact any federal breach law that preempts state breach laws or, especially, preempts other state data security rights or protections: In 2003, when Congress, in the FACT Act, amended the Fair Credit Reporting Act, it specifically did not preempt the right of the states to enact stronger data security and identity theft protections.[11] 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.[12]

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.[13]

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 2003 FACT Act example above.

Simply as an example, S. 961 (Carper) includes sweeping preemption language that is unacceptable to consumer and privacy groups and likely also to most state attorneys general:

> **SEC. 6. 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, communicated, or otherwise handled by, or on behalf of, the person;
> (2) safeguard information relating to consumers from—
> (A) unauthorized access; and
> (B) unauthorized acquisition;

[11] 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/

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

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

(3) investigate or provide notice of the unauthorized acquisition of, or access to, information relating to consumers, or the potential misuse of the information, for fraudulent, illegal, or other purposes; or
(4) mitigate any potential or actual loss or harm resulting from the unauthorized acquisition of, or access to, information relating to consumers.

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.

I would also note that most federal breach proposals define harm very narrowly to financial harm. As we have seen with the latest breaches of health insurance companies, tax preparation firms and the IRS itself, and now even the U.S. OPM, harms from data breaches have gone far beyond existing account fraud or even new account identity theft to include theft of medical services, theft of tax refunds and the reputational and physical threat harms that could result from the OPM breach of security clearance files, including fingerprints.[14] Just a few weeks ago, a national consumer reporting agency, Experian, was even breached, although it states that its credit reports on 200 million Americans were not affected.[15]

In addition, most federal proposals have a weak notice requirement with a risk "trigger" based on a narrow definition of harm. 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, but no other harms.

Only an acquisition standard will 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.

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

[14] I discussed the issue of broad harms and narrow protections in detail here in my blog (24 June 2015): http://uspirg.org/blogs/eds-blog/usp/more-i-hear-about-opm-data-breach-less-i-know-except-its-bad
[15] News release, "PIRG, Others Ask CFPB, FTC to Investigate Experian/T-Mobile Data Breach," 8 October 2015, http://uspirg.org/news/usp/pirgs-others-ask-cfpb-ftc-investigate-experiant-mobile-data-breach

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.

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.[16] Congress 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 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 (merchants) are treated unfairly.

Conclusion:

In conclusion, consumers will benefit from lower fraud risks by the transition to a Chip card regime but the banking industry deserves to be called out for imposing higher Chip reader costs on merchants without also further reducing their fraud risk by rolling out Chip and PIN instead of Chip and signature cards. The liability shift is a big stick, added to numerous other "fee and rule sticks" that the banks already use to extract fees and maintain market power; but the carrot of reducing fraud even further by going with "best available" technology rather than "best for banks" technology would have been a better solution.

I would also note two other impacts on consumers from the transition. First, as the FTC has noted, the rollout is confusing and scam artists are taking advantage of the October 1 date to create new scam pitches to consumers.[17] Another problem I have heard of, although not confirmed, is one that may be faced by consumers traveling in Europe who encounter unattended fare machines that may require a PIN at all times.

.

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

[16] 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

[17] See FTC blog of 19 October 2015, "Scam du jour: Chip card scams," http://www.consumer.ftc.gov/blog/scam-du-jour-Chip-card-scams

HOUSE COMMITTEE ON SMALL BUSINESS
Witness Disclosure Statement
Required by House Rule XI, Clause 2(g)

Your Name: Edmund Mierzwinski		
1. Are you testifying on behalf of a Federal, State, or Local Government entity?	**YES**	**NO** X
2. Are you testifying on behalf of an entity other than a Government entity?	X **YES**	**NO**
3. Other than yourself, please list what entity or entities you are representing: My employer, U.S. Public Interest Research Group, a non-profit consumer group.		
4. Please list any offices or elected positions held or briefly describe your representational capacity with the entities disclosed in question 3. I am employed as Consumer Program Director.		
(For those testifying on behalf of a Government entity, ignore these questions below)		
5. a) Please list any Federal grants or contracts (including subgrants or subcontracts), including the amount and source (agency) which <u>you</u> have received and/or been approved for since January 1, 2013: NONE		
b) If you are testifying on behalf of a non-governmental entity, please list any federal grants or contracts (including subgrants or subcontracts) and the amount and source (agency) received by the <u>entities listed under question 3</u> since January 1, 2013, which exceeded 10% of the entities' revenues in the year received: NONE		
6. If you are testifying on behalf of a non-governmental entity, does it have a parent organization or an affiliate who you specifically do not represent? If so, list below:	**YES**	**NO** X

Signature: Edmund Mierzwinski **Date:** 19 Oct 2015