TESTIMONY OF

MALLORY B. DUNCAN

GENERAL COUNSEL AND SENIOR VICE PRESIDENT,
NATIONAL RETAIL FEDERATION

BEFORE THE SENATE COMMERCE, SCIENCE, AND TRANSPORTATION
SUBCOMMITTEE ON CONSUMER PROTECTION, PRODUCT SAFETY,
INSURANCE AND DATA SECURITY

HEARING ON

"GETTING IT RIGHT ON DATA BREACH AND NOTIFICATION LEGISLATION
IN THE 114TH CONGRESS"

FEBRUARY 5, 2015

National Retail Federation
1101 New York Avenue, NW
Suite 1200
Washington, DC 20005
(202) 626-8126
www.nrf.com

Chairman Moran, Ranking Member Blumenthal, and members of the Subcommittee, on behalf of the National Retail Federation (NRF), I want to thank you for giving us the opportunity to testify at this hearing and provide you with our views on data breach notification legislation and protecting American's sensitive information. NRF is the world's largest retail trade association, representing discount and department stores, home goods and specialty stores, Main Street merchants, grocers, wholesalers, chain restaurants and Internet retailers from the United States and more than 45 countries. Retail is the nation's largest private sector employer, supporting one in four U.S. jobs – 42 million working Americans. Contributing $2.6 trillion to annual GDP, retail is a daily barometer for the nation's economy.

Collectively, retailers spend billions of dollars safeguarding sensitive customer information and fighting fraud. Data security is something that our members strive to improve every day. Virtually all of the data breaches we've seen in the United States during the past year – from attacks on the networked systems of retailers, entertainment and technology companies that have been prominent in the news, to a reported series of attacks on our largest banks that have received less attention – have been perpetrated by criminals that are breaking the law. All of these companies are victims of these crimes and we should keep that in mind as we explore this topic and public policy initiatives relating to it.

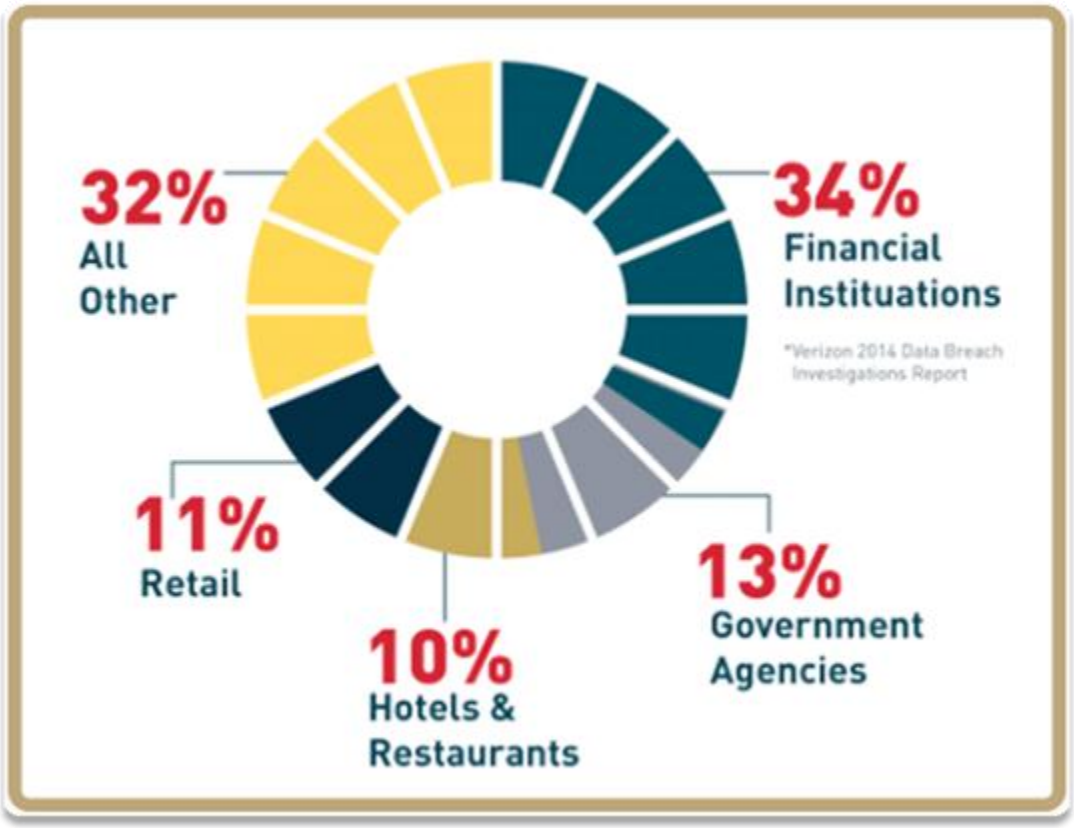
This issue is one that we urge the Committee to examine in a holistic fashion: we need to reduce fraud or other economic harm that may result from a data breach. That is, we should not be satisfied with simply determining what to do after a data breach occurs – that is, who to notify and how to assign liability. Instead, it's important to look at why such breaches occur, and what the perpetrators get out of them, so that we can find ways to reduce and prevent not only the breaches themselves, but the follow-on harm that is often the goal of these events. If breaches become less profitable to criminals, then they will dedicate fewer resources to committing them, and our goals will become more achievable.

With that in mind, these comments are designed to provide some background on data breaches and on fraud, explain how these events impact all business's networked systems, discuss some of the technological advancements retailers have promoted that could improve the security of our networks, offer additional ways to achieve greater payment security, and suggest the elements of data breach notification legislation that may provide the best approach to developing a uniform, nationwide notification standard, based on the strong consensus of state laws, that applies to all businesses that handle sensitive personal information of consumers.

Data Breaches in the United States

Unfortunately, data breaches are a fact of life in the United States, and virtually every part of the U.S. economy and government is being attacked in some way. In its 2014 Data Breach Investigations Report, Verizon determined there were 63,347 data security incidents reported by industry, educational institutions, and governmental entities in 2013, and that 1,367 of those had confirmed data losses. Of those, the financial industry suffered 34%, public institutions (including governmental entities) had 12.8%, the retail industry had 10.8%, and hotels and restaurants combined had 10%. *Figure 1* below illustrates where breaches occur.

Where Breaches Occur *(Figure 1)*



Source: 2014 Data Breach Investigations Report, Verizon[1]

It may be surprising to some, given recent media coverage, that three times more data breaches occur at financial institutions than at retailers. And, it should be noted, even these figures obscure the fact that there are far more merchants that are potential targets of criminals in this area, as there are one thousand times more merchants accepting card payments in the United States than there are financial institutions issuing cards and processing those payments. It is not surprising that the thieves focus far more often on banks, which have our most sensitive financial information – including not just card account numbers but bank account numbers, social security numbers and other identifying data that can be used to steal identities beyond completing some fraudulent transactions.

These figures are sobering. There are far too many breaches. And, breaches are often difficult to detect and carried out in many cases by criminals with real resources behind them. Financially focused crime seems to most often come from organized groups in Eastern Europe rather than state-affiliated actors in China, but the resources are there in both cases. The acute pressure on consumer-serving companies, including those in e-commerce, as well as on our financial system, is due to the overriding criminal goal of financial fraud. We need to recognize that this is a continuous battle against determined fraudsters and be guided by that reality.

[1] 2014 Data Breach Investigations Report by Verizon, available at: http://www.verizonenterprise.com/DBIR/2014/

Breaches Affect Everyone; Federal Legislation Should Be Similarly Comprehensive

The Year of the Breach, as 2014 has been nicknamed, was replete with news stories about data security incidents that raised concerns for all American consumers and for the businesses with which they frequently interact. Criminals focused on U.S. businesses, including merchants, banks, telecom providers, cloud services providers, technology companies, and others. These criminals devoted substantial resources and expertise to breaching the most advanced data protection systems. Vigilance against these threats is necessary, but we need to focus on the underlying causes of breaches as much as we do on the effects of them.

If there is anything that the recently reported data breaches have taught us, it is that any security gaps left unaddressed will quickly be exploited by criminals. For example, the failure of the payment cards themselves to be secured by anything more sophisticated than an easily-forged signature makes the card numbers particularly attractive to criminals and the cards themselves vulnerable to fraudulent misuse. Likewise, cloud services companies that do not remove data when a customer requests its deletion, leave sensitive information available in cloud storage for thieves to later break in and steal, all while the customer suspects it has long been deleted. Better security at the source of the problem is needed. The protection of Americans' sensitive information is not an issue on which unreasonably limiting comprehensiveness makes any sense.

In fact, the safety of Americans' data is only as secure as the weakest link in the chain of entities that share that data for a multitude of purposes. For instance, when information moves across communications lines – for transmission or processing – or is stored in a "cloud," it would be senseless for legislation to exempt these service providers, if breached, from comparable data security and notification obligations to those that the law would place upon any other entity that suffers a breach. Likewise, data breach legislation should not subject businesses handling the same sensitive customer data to different sets of rules with different penalty regimes, as such a regulatory scheme could lead to inconsistent public notice and enforcement.

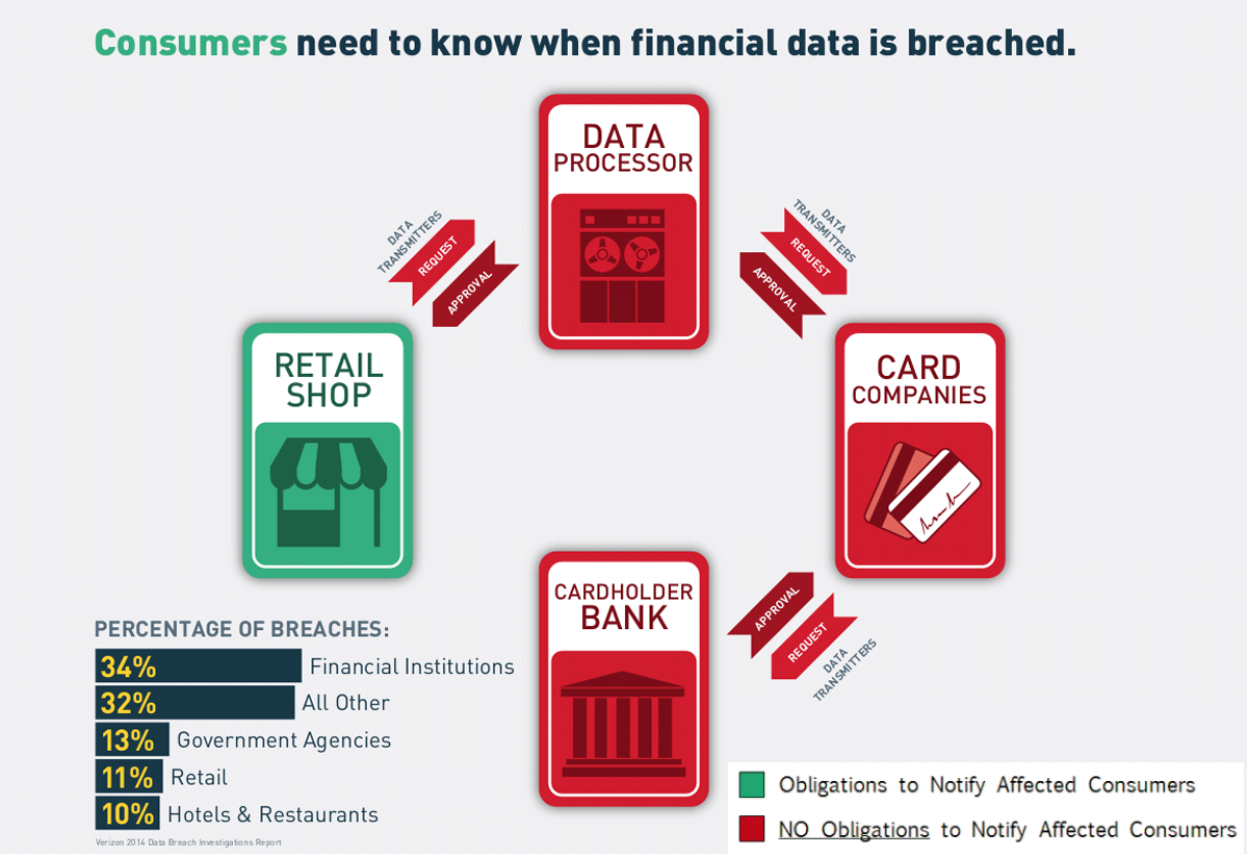
Given the breadth of these invasions, if Americans are to be adequately protected and informed, federal legislation to address these threats must cover all of the types of entities that handle sensitive personal information. Exemptions for particular industry sectors not only ignore the scope of the problem, but create risks criminals can exploit. Equally important, a single federal law applying to all breached entities would ensure clear, concise and consistent notices to all affected consumers regardless of where they live or where the breach occurs.

Third-Party Exemptions

Figure 2, below, illustrates what some legislative proposals, introduced in the last Congress, would require in terms of notice by third parties. This graphic illustrates a typical payment card transaction in which this Committee has jurisdiction over all of the entities except for the bank. In a typical card transaction, a payment card is swiped at a card-accepting business, such as a retail shop, and the information is transmitted via communications carriers to a data processor, which in turn processes the data and transmits it over communications lines to the branded card network, such as Visa or MasterCard, which in turn processes it and transmits it over communications lines to the card-issuing bank. (Typically there also is an acquirer bank

adjacent to the processor in the system, which *figure 2* omits.) Some legislative proposals would only require the retail shop, in this example, to provide notice of a breach of security. The data processor, data transmitter or card company suffering a breach would qualify as a third-party whose only obligation, if breached, is to notify the retail shop of their breach – not affected consumers or the public – so that the retailer provides notice on their behalf. And the bank suffering a breach would be exempt from notifying consumers or the public under most federal legislative proposals to date. Not only does this notice regime present an inaccurate picture to consumers, but it is fraught with possible over-notification because payment processors and card companies are in a one-to-many relationship with retailers. If the retailers must bear the burden for every other entity in the networked system that suffers a breach, then 100% of the notices would come from entities that suffer only 11% of the breaches. This is neither fair nor enlightened public policy.

Notice Obligations <u>Should</u> Apply to All Breached Entities *(Figure 2)*



A recent example illustrates this point about the risk of over-notifying and confusing American consumers if this proposed third-party notice rule illustrated in *Figure 2* is adopted. The largest payment card breach in history occurred at a payment processor, Heartland Payment Systems, which was breached in 2008 resulting in the compromise of over 130 million payment cards. If Heartland had only followed the proposed third-party notice rule in federal legislation, rather than notifying the public of its breach (as it did), it would have only been obligated to

separately notify each of the merchants that it processed payments for, letting them know the affected card numbers that were breached. Those merchants (who were not breached) would, in turn, have to request (and possibly pay for) the contact information for each cardholder through some arrangement with each affected card company or card-issuing bank, and then make notice to those affected customers and/or make "substitute" notice (where individualized notice cannot be made) by announcing the breach to the general public. If affected consumers shopped at a number of retailers that all used the same payment processor that suffered the breach (Heartland, in this hypothetical), the consumers could potentially receive slightly different notices from each store -- all providing what they knew about the breach of the same payment processor – when none of those branded retail stores actually suffered the breach itself. This proposal creates an untenable public policy solution that neither serves consumers nor businesses that have secured their own networks.

Just as merchants, such as Target, who have publicly acknowledged a breach have taken tremendous steps to heighten their security, Heartland continued to harden its systems (after notifying of its own breach) and now is recognized as one of the most secure platforms in the industry. The threat of public notice has had a multiplier effect on other commercial businesses.

Indeed, Congress could go further: it could establish the same data breach notice obligations for *all* entities handling sensitive data that suffer a breach of security. Congress should not permit "notice holes" – the situation where certain entities are exempt from reporting known breaches of their own systems. If we want meaningful incentives to increase security, everyone needs to have skin in the game.

Financial Institution Exemptions

Many legislative proposals last Congress, however, had "notice holes," where consumers would not receive disclosures of breaches by certain entities. Perhaps the notice hole that has been left unplugged in most proposals is the exemption from notification standards for entities subject to the Gramm Leach Bliley Act (GLBA), which itself does not contain any statutory language that requires banks to provide notice of their security breaches to affected consumers or the public. Interpretive information security guidelines issued by federal banking regulators in 2005 did not address this lack of a requirement when it set forth an essentially precatory standard for providing consumer notice in the event banks or credit unions were breached. Rather, the 2005 interagency guidelines state that banks and credit unions "should" conduct an investigation to determine whether consumers are at risk due to the breach and, if they determine there is such a risk, they "should" provide consumer notification of the breach.[2] These guidelines fall short of creating a notification requirement using the language of "shall," an imperative command used in proposed breach notification legislation for entities that would be subject to Federal Trade Commission enforcement. Instead, banks and credit unions are left to make their own determinations about when and whether to inform consumers of a data breach.

[2] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736 (Mar. 29, 2005) promulgating 12 C.F.R. Part 30, app. B, Supplement A (OCC); 12 C.F.R. Part 208, app. D-2, Supplement A and Part 225, app. F, Supplement A (Board); 12 C.F.R. Part 364, app. B, Supplement A (FDIC); and 12 C.F.R. Part 570, app. B, Supplement A (OTS), accessible at: https://www.fdic.gov/news/news/financial/2005/fil2705.html.

Several accounts in 2014 of breaches at the largest U.S. banks demonstrate the lack of any notice requirement under the interagency guidelines. It was reported in news media last Fall that as many as one dozen financial institutions were targeted as part of the same cyber-attack scheme.[3] It is not clear to what extent customers of many of those institutions had their data compromised, nor to our knowledge have the identities of all of the affected institutions been made public The lack of transparency and dearth of information regarding these incidents reflects the fact that banks are not subject to the same requirements to notify affected customers of their own breaches of security as other businesses are required now under 47 state laws and would be required under most proposed federal legislation, despite the fact that financial institutions hold Americans' most sensitive financial information. A number of the more seasoned and robust state laws, such as California's breach notification law, have not exempted financial institutions from their state's breach notification law because they recognize that banks are not subject to any federal requirement that says they "shall" notify customers in the event of a breach of security.

Service Provider Exemptions

Another notice hole that has remained unplugged in legislative proposals for many years is the service provider breach exemption, similar to the bank breach exemption, that would permit an entity providing data transmission or storage services to avoid providing consumer or public notice when it is aware of a breach of its data system. Other businesses, such as retailers, are required to provide notice even if they don't have the contact information for the affected consumers. The service provider exemption would, however, permit no notice at all to be made, not even to the FTC or law enforcement for a known breach of security affecting sensitive personal information. Surely Congress should not pass a disclosure law that provides a free pass for known breaches of security to certain service providers simply because they have successfully had such an exemption inserted into some past legislative proposals. Allowing this type of hole in notice requirements does not make sense. Just because a telecommunications provider, cloud data service, payment processor or other company provides a service to another business does not mean it should not have to provide notice of its data breaches. With an exemption for service providers like these, there is real risk that the public won't get information it needs and/or that other businesses will have to plug the gap and take the attendant cost and blame for someone else's data breach. And, of course, such a scheme would not create the incentives for service providers to improve their data security systems.

General Principle for Notification

With respect to establishing a national standard for individual notice in the event of a breach of security at an entity handling sensitive personal information, the only principle that makes sense is that these breached entities should be obligated to notify affected individuals or make public notice when they discover breaches of their own systems. Just as the Federal Trade Commission (FTC) expects there to be reasonable data security standards employed by each business that handles sensitive personal information, a federal breach notification bill should apply notification standards that "follow the data" and apply to any entity in a networked system

[3] "JP Morgan Hackers Said to Probe 13 Financial Firms," *Bloomberg* (Oct. 9, 2014).

that suffers a breach of security when sensitive data is in its custody. With respect to those who have called upon the entity that is "closest to the consumer" to provide the notice, we would suggest that the one-to-many relationships that exist in the payment card system and elsewhere will ultimately risk having multiple entities all notify about the same breach – someone else's breach. This is not the type of transparent disclosure policy that Congress has typically sought. An effort to promote relevant notices should not obscure transparency as to where a breakdown in the system has occurred. Indeed, a public notice obligation on all entities handling sensitive data would create significant incentives for every business that operates in our networked economy to invest in reasonable data security to protect the sensitive data in its custody. By contrast, a federal law that permits "notice holes" in a networked system of businesses handling the same sensitive personal information – requiring notice of some sectors, while leaving others largely exempt – will unfairly burden the former and unnecessarily betray the public's trust.

More than 50 U.S. Jurisdictions Have Notice Laws; Congress Should Step in Now to Establish a Nationwide, Uniform Standard to Benefit Both Consumers and Businesses

For more than a decade, the U.S. federalist system has enabled every state to develop its own set of disclosure standards for companies suffering a breach of data security and, to date, 47 states and 4 other federal jurisdictions (including the District of Columbia and Puerto Rico) have enacted varying data breach notification laws. Many of the states have somewhat similar elements in their breach disclosure laws, including definitions of covered entities and covered data, notification triggers, timeliness of notification, provision specifying the manner and method of notification, and enforcement by state attorneys general. But they do not all include the same requirements, as some cover distinctly different types of data sets, some require that particular state officials be notified, and a few have time constraints (although the vast majority of state laws only require notice "without unreasonable delay" or a similar phrase.)

Over the past ten years, businesses such as retailers, to whom all the state and federal territory disclosure laws have applied, have met the burden of providing notice, even when they did not initially have sufficient information to notify affected individuals, through standardized substitute notification procedures in each state law. However, with an increasingly unwieldy and conflicting patchwork of disclosure laws covering more than 50 U.S. jurisdictions, it is time for Congress to acknowledge that the experimentation in legislation that is at the state level that defines our federalist system has reached its breaking point, and it is time for Congress to the step in to create a national, uniform standard for data moving in interstate commerce in order to ensure uniformity of a federal act's standards and the consistency of their application across jurisdictions.

For years, NRF has called on Congress to enact a preemptive federal breach notification law that is modeled upon the strong consensus of existing laws in nearly every state, the District of Columbia, Puerto Rico and other federal jurisdictions. A single, uniform national standard for notification of consumers affected by a breach of sensitive data would provide simplicity, clarity and certainty to both businesses and consumers alike. Importantly, a single federal law would permit companies victimized by a criminal hacking to devote greater attention in responding to such an attack to securing their networks, determining the scope of affected data, and identifying

the and customers to be notified, rather than diverting limited time and resources to a legal team attempting to reconcile a patchwork of conflicting disclosure standards in over 50 jurisdictions. In sum, passing a federal breach notification law is a common-sense step that Congress should take now to ensure reasonable and timely notice to consumers while providing clear compliance standards for businesses.

Preemption of state laws and common laws that create differing disclosure standards is never easy, and there is a long history of Supreme Court and other federal courts ruling that, even when Congress expresses an intent to preempt state laws, limiting the scope of the preemption will not result in preemption. All it will accomplish is to add yet another law, this time federal, to the state statutes and common laws already in effect, resulting in the continuation of a confusing tapestry of state law requirements and enforcement regimes. A federal act that leaves this in place would undermine the very purpose and effectiveness of the federal legislation in the first place.

In order to establish a uniform standard, preemptive federal legislation is necessary. But that does not mean (as some have contended) that the federal standard must or should be "weaker" than the state laws it would replace. On the contrary, in return for preemption, the federal law should reflect a strong consensus of the many state laws. Some have called for a more robust notification standard at the federal level than exists at the state level. Without adding unnecessary bells and whistles, NRF believes that Congress can create a stronger breach notification law by removing the exemptions and closing the types of "notice holes" that exist in several state laws, thereby establishing a breach notification standard that applies to all businesses – as this Committee has done in previous consumer protection legislation that is now federal law. This approach would enable members that are concerned about preempting state laws to do so with confidence that they have created a more transparent and better notification regime for consumers and businesses alike. It is a way this Committee and Congress can work to enact a law with both robust protection and preemption.

We urge you, therefore, in pursuing enactment of federal breach notification legislation, to adopt a framework that applies to all entities handling sensitive personal information in order to truly establish uniform, nationwide standards that lead to clear, concise and consistent notices to all affected consumers whenever or wherever a breach occurs. When disclosure standards apply to all businesses that handle sensitive data, it will create the kind of security-maximizing effect that Congress wishes to achieve.

Multi-Tiered Set of Data Security Standards Applicable to Retailers

Theoretically, security is like defense. One could spend all one's money on defense and still not be 100% protected. In the real world it is even more difficult.

Federal and State Data Security Standards

Data security standards vary depending on the nature of an entity's business and where it operates. Over the past half-century, the United States has essentially taken a sector-specific approach to data privacy (including data security) requirements, and our current legal framework

reflects this. For example, credit reporting agencies, financial institutions, and health care providers, just to name a few regulated sectors, have specific data security standards that flow from laws enacted by Congress, such as the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act (HIPAA), respectively. Those operating in other industry sectors that are subject to the jurisdiction of the Federal Trade Commission (FTC) must abide by the standards of care enforced by the FTC under Section 5 of the FTC Act, which give the Commission broad, discretionary authority to prosecute "unfair or deceptive acts or practices" (often referred to as their "UDAP" authority). On top of this federal statutory and regulatory framework, states have regulated businesses' data security practices across a variety of industry sectors and enforced consumer protection laws through their state consumer protection agencies and/or their attorneys general.

Legal exposure for data security failures is dependent on the federal or state laws to which a business may be subject and is alleged to violate. The FTC, for example, has been very active in bringing over 50 actions against a range of companies nationwide that are not otherwise subject to a sector-specific federal data security law (e.g., GLBA, HIPAA, etc.). For example, under its Section 5 UDAP authority, the FTC has brought enforcement actions against entities that the Commission believes fall short in providing "reasonable" data security for personal information. Nearly all of these companies have settled with the FTC, paid fines for their alleged violations (sometimes to the extent of millions of dollars), and agreed to raise their security standards and undergo extensive audits of their practices over the next several decades to ensure that their data security standards are in line with the FTC's order.

Effect of Imposing GLBA-Like Standards with FTC Enforcment

Providing the FTC, however, with the authority to enforce discretionary data security standards like those in the GLBA guidelines would dramatically expand FTC authority. Banking regulators take an audit/examination approach to regulating companies and work with them through an iterative process to help the institution come into compliance where it may be lacking without the threat of severe penalties. The FTC, by contrast, takes an enforcement approach, which under a GLBA guidelines standard, would require a post-hoc determination of a company's compliance with an amorphous standard in a world where the technological threat vectors are ever-changing. In an enforcement approach, entities are either guilty or not, and more often guilty by the mere fact of a breach; unlike with GLBA guidelines, companies regulated by the FTC are not able to get several bites at the apple working with regulators until they know they are in compliance with the regulator's vision for the rule. Companies regulated by the FTC would have to guess at what will satisfy the agency and, if their security is breached, the strong enforcement presumption would be that the company failed to meet the standard.

The different enforcement regimes between financial institutions and entities subject to the FTC's jurisdiction is also evident in the manner and frequency with which fines are assessed and civil penalties imposed for non-compliance with a purported data security standard. Banks are rarely (if ever) fined by their regulators for data security weaknesses. But, as noted, commercial companies have been fined repeatedly by the FTC. Providing an agency like the FTC, with an enforcement approach, a set of standards with significant room for interpretation is

likely to lead to punitive actions that are different in kind and effect on entities within the FTC's jurisdiction than the way the standards would be utilized by banking regulators in an examination. A punitive approach to companies already victimized by a crime would not be appropriate nor constructive in light of the fact that the FTC itself has testified before this Committee that no system – even the most protected one money can buy – is ever 100% secure.

Improving Payment Card Security

Using the best data security technology and practices available still does not guarantee that a business can avoid suffering a data security breach. Therefore, raising security standards alone may not be the most efficient or effective means of preventing potential harm to consumers. With respect to payment card numbers, for example, it is possible that no matter how much security is applied by a business storing these numbers, the numbers may be stolen from a business's database in a highly sophisticated security breach that can evade even state-of-the-art system security measures. Because of these risks, it makes sense for industry to do more than just apply increased network or database security measures. One sensible proposal is to minimize the storage by businesses of the full set of unredacted and unencrypted payment card numbers necessary to complete a transaction – a data protection principle known as "data minimization." Another method to help prevent downstream fraud from stolen card numbers is to require more data or numbers (such as a 4-digit PIN) from a consumer than simply the numbers that appear on a card to authorize and complete payment card transactions.

For example, a decade ago, the National Retail Federation asked the branded card networks and banks to lift the requirement that retailers store full payment card numbers for all transactions. Retailers have also pushed to phase-out signature-authentication for cards and, instead, use a more secure authentication method for credit and debit card transactions, such as the PIN-based authentication that banks require for accessing bank accounts through ATM machines. PINs can provide an extra layer of security against downstream fraud even if the card numbers (which the card companies already emboss on the outside of a card) are stolen in a breach. In PIN-based transactions, for example, the stored 20-digits from the card would, alone, be insufficient to conduct a fraudulent transaction in a store without the 4-digit PIN known to the consumer and not present on the card itself. These business practice improvements are easier and quicker to implement than any new federal data security law, and they hold the promise of being more effective at preventing the kind of financial harm that could impact consumers as companies suffer data security breaches affecting payment cards in the future.

On October 17, 2014, the President signed an executive order initiating the BuySecure Initiative for government payment cards.[4] The order provided, among other things, that payment cards issued to government employees would include PIN and chip technology and that government equipment to handle and process transactions would be upgraded to allow acceptance of PIN and chip. These are common-sense actions that recognize that while it may not be possible to ensure there is never another data security breach, it is still possible to

[4] Executive Order --Improving the Security of Consumer Financial Transactions, The White House, October 17, 2014. Accessible at: http://www.whitehouse.gov/the-press-office/2014/10/17/executive-order-improving-security-consumer-financial-transactions

minimize the harms that can come from those breaches – and reduce the incentives from criminals to try to steal some data in the first place.

PCI-DSS Standards

When it comes to protecting payment card data, however, retailers are essentially at the mercy of the dominant credit card companies. The credit card networks – Visa, MasterCard, American Express, Discover and JCB – are responsible for an organization known as the PCI (which stands for "Payment Card Industry") Data Security Council. PCI establishes data security standards (PCI-DSS) for payment cards. While well-intentioned in concept, these standards have not worked quite as well in practice. They have been inconsistently applied, and their avowed purpose has been significantly altered.

PCI has, in critical respects over time, pushed card security costs onto merchants even when other decisions might have more effectively reduced fraud – or done so at lower cost. For example, retailers have long been required by PCI to encrypt the payment card information that they have. While that is appropriate, PCI has not required financial institutions to be able to accept that data in encrypted form. That means the data often has to be de-encrypted at some point in the process in order for transactions to be processed.

Similarly, merchants are expected to annually demonstrate PCI compliance to the card networks, often at considerable expense, in order to benefit from a promise that the merchants would be relieved of certain fraud inherent in the payment system, which PCI is supposed to prevent. However, certification by the networks as PCI Compliant apparently has not been able to adequately contain the growing fraud and retailers report that the "promise" increasingly has been abrogated or ignored. Unfortunately, as card security expert Avivah Litan of Gartner Research wrote recently, "The PCI (Payment Card Industry) security standard has largely been a failure when you consider its initial purpose and history."[5]

Retailers have spent billions of dollars on card security measures and upgrades to comply with PCI card security requirements, but it hasn't made them immune to data breaches and fraud. The card networks have made those decisions for merchants and the increases in fraud demonstrate that their decisions have not been as effective as they should have been.

Improving Technology Solutions to Better Protect Consumers in Payment Transactions

PIN-Authentication of Cardholders

There are technologies available that could reduce fraud. An overhaul of the fraud-prone cards that are currently used in the U.S. market is long overdue. As I noted, requiring the use of a PIN is one way to reduce fraud. Doing so takes a vulnerable piece of data (the card number) and makes it so that it cannot be used on its own. This ought to happen not only in the brick-and-mortar environment in which a physical card is used but also in the online environment in which the physical card does not have to be used. Many U.S. companies, for example, are

[5] "How PCI Failed Target and U.S. Consumers," by Avivah Litan, Gartner Blog Network, Jan. 20, 2014, available at http://blogs.gartner.com/avivah-litan/2014/01/20/how-pci-failed-target-and-u-s-consumers/.

exploring the use of a PIN for online purchases. This may help directly with the 90 percent of U.S. fraud which occurs online. It is not happenstance that automated teller machines (ATMs) require the entry of a PIN before dispensing cash. Using the same payment cards for purchases should be just as secure as using them at ATMs.

End-to-End Encryption

Another technological solution that could help deter and prevent data breaches and fraud is encryption. Merchants are already required by PCI standards to encrypt cardholder data but, not everyone in the payments chain is required to be able to accept data in encrypted form. That means that data may need to be de-encrypted at some points in the process. Experts have called for a change to require "end-to-end" (or point-to-point) encryption which is simply a way to describe requiring everyone in the payment-handling chain to accept, hold and transmit the data in encrypted form.

According to the September 2009 issue of the Nilson Report "most recent cyberattacks have involved intercepting data in transit from the point of sale to the merchant or acquirer's host, or from that host to the payments network." The reason this often occurs is that "data must be decrypted before being forwarded to a processor or acquirer because Visa, MasterCard, American Express, and Discover networks can't accept encrypted data at this time."[6]

Keeping sensitive data encrypted throughout the payments chain would go a long way to convincing fraudsters that the data is not worth stealing in the first place – at least, not unless they were prepared to go through the arduous task of trying to de-encrypt the data which would be necessary in order to make use of it. Likewise, using PIN-authentication of cardholders now would offer some additional protection against fraud should this decrypted payment data be intercepted by a criminal during its transmission "in the clear."

Tokenization and Mobile Payments

Tokenization is another variant that could be helpful. Tokenization is a system in which sensitive payment card information (such as the account number) is replaced with another piece of data (the "token"). Sensitive payment data could be replaced with a token to represent each specific transaction. Then, if a data breach occurred and the token data were stolen, it could not be used in any other transactions because it was unique to the transaction in question. This technology has been available in the payment card space since at least 2005.[7] Still, tokenization is not a panacea, and it is important that whichever form is adopted be an open standard so that a small number of networks not obtain a competitive advantage, by design, over other payment platforms

In addition, in some configurations, mobile payments offer the promise of greater security as well. In the mobile setting, consumers won't need to have a physical card – and they certainly won't replicate the security problem of physical cards by embossing their account

[6] The Nilson Report, Issue 934, Sept. 2009 at 7.
[7] For information on Shift4's 2005 launch of tokenization in the payment card space see http://www.internetretailer.com/2005/10/13/shift4-launches-security-tool-that-lets-merchants-re-use-credit.

numbers on the outside of their mobile phones. It should be easy for consumers to enter a PIN or password to use payment technology with their smart phones. Consumers are already used to accessing their phones and a variety of services on them through passwords. Indeed, if we are looking to leapfrog the already aging current technologies, mobile-driven payments may be the answer.

Indeed, as much improved as they are, the proposed chips to be slowly rolled out on U.S. payment cards are essentially dumb computers. Their dynamism makes them significantly more advanced than magstripes, but their sophistication pales in comparison with the common smartphone. Smartphones contain computing powers that could easily enable comparatively state-of-the-art fraud protection technologies. In fact, "the new iPhones sold over the weekend of their release in September 2014 contained 25 times more computing power than the whole world had at its disposal in 1995."[8] Smart phones soon may be nearly ubiquitous, and if their payment platforms are open and competitive, they will only get better.

The dominant card networks have not made all of the technological improvements suggested above to make the cards issued in the United States more resistant to fraud, despite the availability of the technology and their adoption of it in many other developed countries of the world, including Canada, the United Kingdom, and most countries of Western Europe.

In this section, we have merely described some of the solutions available, but the United States isn't using any of them the way that it should be. While everyone in the payments space has a responsibility to do what they can to protect against fraud and data theft, the card networks have arranged the establishment of the data security requirements and yet, in light of the threats, there is much left to be desired.

Legislative Solutions Beyond Breach Notification

In addition to the marketplace and technological solutions suggested above, NRF also supports a range of legislative solutions that we believe would help improve the security of our networked systems, ensure better law enforcement tools to address criminal intrusions, and standardize and streamline the notification process so that consumers may be treated equally across the nation when it comes to notification of data security breaches.

Legislation Protecting Consumers' Debit Cards to the Same Extent as Credit Cards

From many consumers' perspective, payment cards are payment cards. As has been often noted, consumers would be surprised to learn that their legal rights, when using a debit card – i.e., their own money – are significantly less than when using other forms of payment, such as a credit card. It would be appropriate if policy makers took steps to ensure that consumers' reasonable expectations were fulfilled, and they received at least the same level of legal protection when using their debit cards as they do when paying with credit.

NRF strongly supports legislation like S. 2200, the "Consumer Debit Card Protection Act," cosponsored by Senators Warner and Kirk last Congress. S. 2200 was a bipartisan solution

[8] "The Future of Work: There's an app for that," *The Economist* (Jan. 3, 2015).

that would immediately provide liability protection for consumers from debit card fraud to the same extent that they are currently protected from credit card fraud. This is a long overdue correction in the law and one important and productive step Congress could take immediately to protect consumers that use debit cards for payment transactions.

Legislation Protecting Businesses that Voluntarily Share Cyber-Threat Information

In addition, NRF supports the passage by Congress of legislation like H.R. 624, the "Cyber Intelligence Sharing and Protection Act," cosponsored last Congress by Congressmen Rogers and Ruppersberger, and which passed the House of Representatives with bipartisan support. This legislation would protect and create incentives for private entities in the commercial sector to lawfully share information about cyber-threats with other private enties and the federal government in real-time. This would help companies better defend their own networks from cyber-attacks detected elsewhere by other business.

Legislation Aiding Law Enforcement Investigation and Prosecution of Breaches

We also support legislation that would provide more tools to law enforcement to ensure that unauthorized network intrusions and other criminal data security breaches are thoroughly investigated and prosecuted, and that the criminals that breach our systems to commit fraud with our customers' information are swiftly brought to justice.

Conclusion

In summary, a federal breach notification law should contain three essential elements:

1. **Uniform Notice**: Breached entities should be obligated to notify affected individuals or make public notice when they discover breaches of their own systems. A federal law that permits "notice holes" in a networked system of businesses handling the same sensitive personal information – requiring notice of some sectors, while leaving others largely exempt – will unfairly burden the former and unnecessarily betray the public's trust.

2. **Express Preemption of State Law**: A single, uniform national standard for notification of consumers affected by a breach of sensitive data would provide simplicity, clarity and certainty to both businesses and consumers alike. Passing a federal breach notification law is a common-sense step that Congress should take now to ensure reasonable and timely notice to consumers while providing clear compliance standards for businesses.

3. **Reflect the Strong Consensus of State Laws**: A national standard should reflect the strong consensus of state law provisions. NRF believes that Congress can create a stronger breach notification law by removing the exemptions and closing the types of "notice holes" that exist in several state laws, thereby establishing a breach notification standard that applies to all businesses, similar to the comprehensive approach this Committee has taken in previous consumer protection legislation that is now federal law.

Appendix:

What Retailers Want You To Know About Data Security[9]

[9] Slides Available at: http://www.slideshare.net/NationalRetailFederation/thingsto-know-datasecurity?ref=https://nrf.com/media/press-releases/retailers-reiterate-support-federal-data-breach-notification-standard

What retailers want you to know about.....

DATA SECURITY

NRF NATIONAL RETAIL FEDERATION

BREAKDOWN

What is a data breach?

A data breach is the unauthorized acquisition of sensitive personal information in digital, electronic or computerized form that creates a risk of financial harm to a consumer.

NRF NATIONAL RETAIL FEDERATION

ISSUE

Who is breaching?

Cybercriminals are constantly trolling for financial data in order to steal card numbers and convert them into cash.

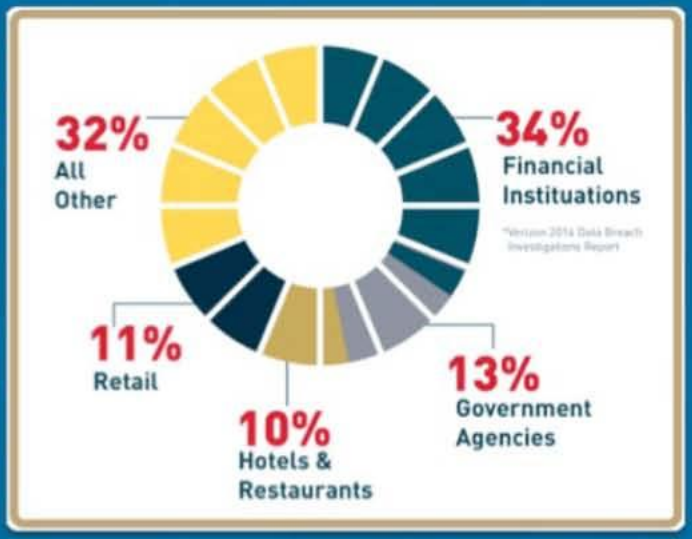
NRF NATIONAL RETAIL FEDERATION

ABOUT

Where do breaches happen?

Hackers don't discriminate – data breaches have targeted a wide variety of businesses from the entertainment industry to financial services.

According to Verizon, retail represents 11 percent of data breaches while the financial services industry accounts for 34 percent.



NRF NATIONAL RETAIL FEDERATION

ABOUT

Why retailers care about data security.

As a consumer-facing and reliant industry, retailers and merchants value every interaction with their customers.

Retailers work every single day and make significant contributions and investments in data, information and payment security to ensure that the retail-customer relationship is secure and protected.

NRF NATIONAL RETAIL FEDERATION

PROBLEM

Cards are fraud prone

The thief creates a duplicate card, signs your name and makes a purchase.

The thief uses your card, signs your name and makes a purchase.

NRF NATIONAL RETAIL FEDERATION

SOLUTION

PIN-and-Chip

Since 2005, the National Retail Federation has urged banks and payment card companies to switch to more secure PIN-and-chip cards, which replace the magnetic stripe with a computer microchip and replace the signature with a Personal Identification Number(PIN) to better protect consumers' financial data when they shop.

The new credit cards being issued this year need to have both a chip and a PIN, not just a chip as proposed by most banks and credit unions. The chip ensures that the card is the one issued by the bank but the PIN is needed to ensure that the person using the card is the actual cardholder and not a thief who stole your chip card.

NRF NATIONAL RETAIL FEDERATION

SOLUTION

PIN and CHIP

Only you know your PIN, so the thief can't enter it to complete an in-store transaction.

The thief cannot duplicate your chip card.

MAGNETIC STRIPE and SIGNATURE

The thief uses your card, signs your name, and makes a purchase.

The thief creates a duplicate card, signs your name, and makes a purchase.

The safest cards deploy both PIN and Chip technology.

PIN and Chip is widely used around the world with great success; the United Kingdom saw a 75% drop in credit card fraud after implementation.*

American consumers deserve better.

*Source: Financial Fraud Action UK

NRF NATIONAL RETAIL FEDERATION

PROBLEM

Cyber-Threat Information Sharing

Congress must pass laws that make it easier for companies to share information and emerging threats without hesitation.

NRF NATIONAL RETAIL FEDERATION

SOLUTION

NRF's Efforts to Improve Threat Information Sharing

To help fight cybersecurity threats to retailers' systems, NRF created the Information Technology Security Council, which keeps retailers up-to-date on the latest news, information and threats. More than 150 retail companies are actively involved.

NRF NATIONAL RETAIL FEDERATION

PROBLEM

Notification isn't uniform

For the past decade, NRF has called for a uniform nationwide data breach notification standard that would preempt the patchwork of 47 state laws. This uniform federal law should be based on and reflect the strong consensus of state laws.

The current patchwork of state and local data breach notice laws with conflicting requirements doesn't work because it diverts limited resources that should be focused on restoring the integrity of a breached system.

NRF NATIONAL RETAIL FEDERATION

SOLUTION

Data Breach Notification Law

A nationwide breach notification law must preempt state and local laws so businesses and consumers understand what disclosures are expected regardless of when or where breaches occur.

Data breach notification should be appropriate, reasonable, relevant and timely.

Federal data breach notification requirements should be comprehensive and apply to every entity that maintains or transmits sensitive information, not just retailers.

NRF NATIONAL RETAIL FEDERATION

PROBLEM

Industries are held to different standards

Merchants have multiple tiers of data security standards. These include Payment Card Industry standards for all merchants accepting payment cards, as well as specific state standards to protect sensitive information. The Federal Trade Commission also enforces federal standards that require all merchants to have reasonable data security protections.

Other breached entities just need to follow industry-specific guidance.

NRF NATIONAL RETAIL FEDERATION

SOLUTION

Cover all entities involved in data breach

A data breach notification law should cover the entire payments system from card companies to telecommunications firms without exception or exemption. Arbitrary timeframes or industry-specific requirements that cover only certain entities should not be established.

NRF NATIONAL RETAIL FEDERATION


Learn more: nrf.com/datasecurity
NRF
NATIONAL
RETAIL
FEDERATION