TESTIMONY OF

MALLORY B. DUNCAN

GENERAL COUNSEL AND SENIOR VICE PRESIDENT,
NATIONAL RETAIL FEDERATION

BEFORE THE HOUSE ENERGY AND COMMERCE COMMITTEE
SUBCOMMITTEE ON COMMERCE, MANUFACTURING AND TRADE

HEARING ON

"DISCUSSION DRAFT OF H.R. ___, DATA SECURITY AND
BREACH NOTIFICATION ACT OF 2015"

MARCH 18, 2015

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

TESTIMONY OF

MALLORY B. DUNCAN

GENERAL COUNSEL AND SENIOR VICE PRESIDENT, NATIONAL RETAIL FEDERATION

Chairman Burgess, Ranking Member Schakowsky, 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 legislation and, more particularly, on the Subcommittee's "discussion draft" of the Data Security and Breach Notification Act of 2015.

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.

At the outset, NRF would like to thank the members of the Subcommittee and staff for the considerable time and effort they have expended to address this critically important issue to our nation's businesses and consumers. Through this hard work, the Committee on Energy and Commerce is beginning to take steps necessary to help raise the level of data security practices throughout industry and to provide greater consumer awareness and notification of breaches of security when they do occur.

We have spent a great deal of time working with our member companies to present the Subcommittee staff with the retail industry perspective on elements of data security and breach notification since the release of the initial draft bill last summer. We view today's hearing as an opportunity to continue a productive dialogue on how the discussion draft today can be further clarified and improved in substantive respects.

We look forward to working with the Subcommittee members as the bill moves through the upcoming markup and onto the next stages of consideration at the full committee level to help ensure that the legislation ultimately reported by the Committee is as strong and effective as it can be. We also trust that the Subcommittee views the analysis of the discussion draft text we provide in this this testimony in the constructive light in which it is intended.

Executive Summary

Maintaining customers' trust is our members' highest priority and, as further detailed in the testimony below, retailers make significant investments in data security with the goal of preventing theft or fraudulent use of customer information. On behalf of our members, NRF has adopted a multi-pronged effort to help improve data security practices, retire fraud-prone payment cards and help in the fight to defend against cyber attacks that threaten all businesses, including retailers. Specifically, these efforts includes support for the establishment of a uniform nationwide breach notification standard, promotion of improved payment card security – such as efforts make PIN and chip cards a reality in the United States – and the programs NRF launched 9 months ago to provide our members with a cybersecurity threat information-sharing and a security alert listserv to help disseminate information that could help prevent cyber attacks.

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.

Additionally, while 51 different U.S. breach notification laws is a nearly nationwide disclosure regime, it is not *uniform,* and it has resulted in a patchwork of notice and other requirements that is neither the most efficient for victimized businesses nor the most effective for consumers. Laws in 47 states and 4 federal jurisdictions (including the District of Columbia) create difficult compliance for our members, particularly mid-sized regional operations that may operate in several states. That is because the applicable state breach notice law is determined by the affected customer's residence, and not the location of the business. The same is true for small and moderately sized online retailers that may have a regional or national footprint. One, uniform nationwide notice standard would help both businesses and consumers by aiding in the provision of effective notice to them when a breach occurs.

Our support for data security breach notification legislation, however, goes beyond support simply for uniformity in application of the law across the United States, as NRF has called for such a law to apply to <u>all</u> businesses that handle sensitive personal information. Establishment of one federal disclosure standard for all businesses handling sensitive customer data will lead to clear, concise and consistent notices to all affected consumers whenever or wherever a breach occurs.

Furthermore, when disclosure standards apply to all businesses that handle sensitive data, it creates the kind of security-maximizing effect that Congress wishes to achieve because all businesses are incentivized to provide greater security in order to avoid public notification of a breach. Exemptions for particular industry sectors would not only ignore the scope of the problem, but create risks criminals can exploit, and disincentives for exempted businesses from making the necessary investment and commitment to improving its data security, because there is no threat of exposure for failures to protect sensitive customer information.

Each of these issues is discussed in greater detail in our written testimony below. To summarize our position on breach notification legislation, NRF has adopted three principles we believe are essential for any proposed federal legislation, as follows:

NRF's 3 Principles for a Federal Breach Notification Law

1. One federal breach notification law that applies to all entities handling sensitive customer data and that establishes the same or similar notice obligations across industry sectors for data breaches;

2. A federal law whose provisions reflect the strong consensus of state laws and, where possible, improve upon deficiencies in those laws that lead to ineffective consumer notice; and

3. A federal law that establishes a uniform, nationwide standard by being truly preemptive of related state laws.

We will offer our more considered views on each of these principles below and, using them as a benchmark, will provide our initial comments on the effectiveness of the discussion draft's provisions to achieve these goals, particularly in the area of notification and preemption. Lastly, we will address the multi-tiered set of data security standards already applying to retailers and ways that retailers are implementing new technologies to help improve the security of their own networks and encourage similar improvements in payment card security used in payment networks not controlled by merchants.

Lastly, before we begin the specific comments on the sections of the bill that relate to our three principles above, we want to first acknowledge and observe that the Subcommittee has addressed previous concerns raised with last summer's draft bill, through textual revisions, so that the current discussion draft features:

- a more carefully-crafted definition of "covered entity" that includes only entities under the Committee's jurisdiction;

- a definition of "service provider" limited to entities subject to the Communications Act; and

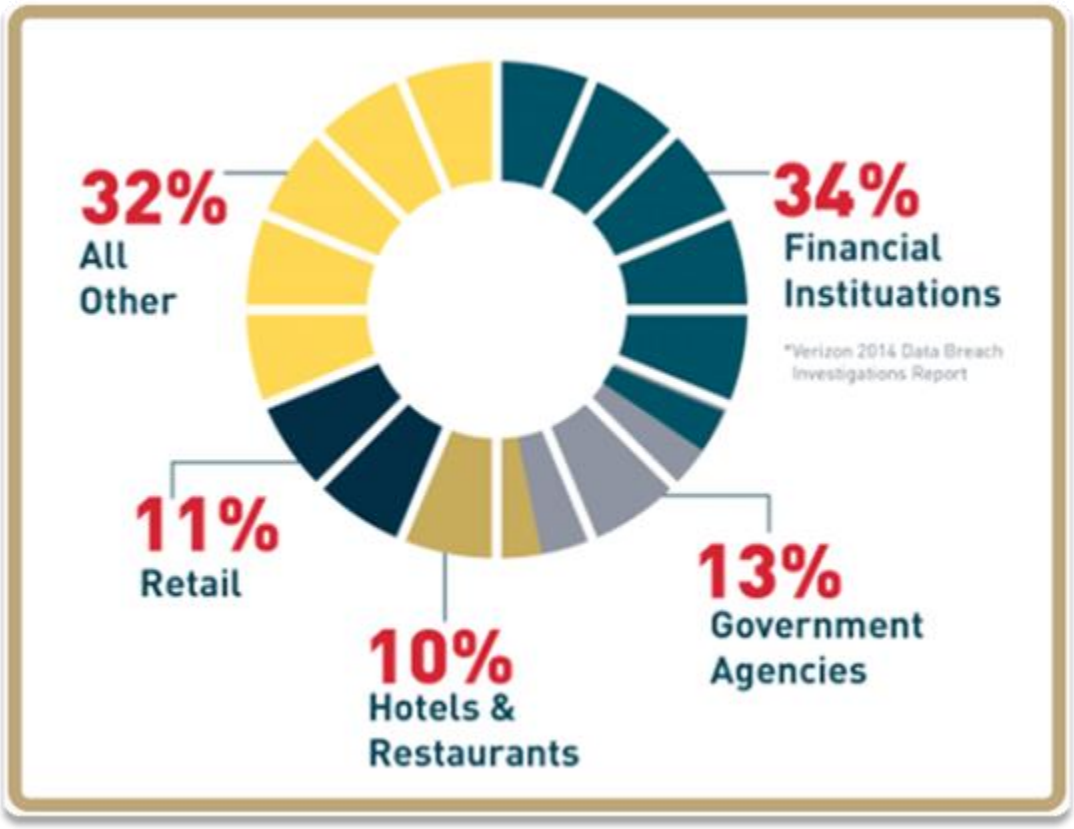
- a revised preemption clause that would not give the benefit of preemption to those who are not subject to bill's obligations.

Legislation Should Require Effective Breach Notice by All Entities Handling Sensitive Data

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 data security breaches. These breaches are often difficult to detect and are carried out in many cases by criminals with significant resources behind them. The acute pressure on consumer-serving companies, including those in

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

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.

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. We live in a networked world. 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 entities, if breached, from comparable data security and notification obligations applying to all other entities that may suffer 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.

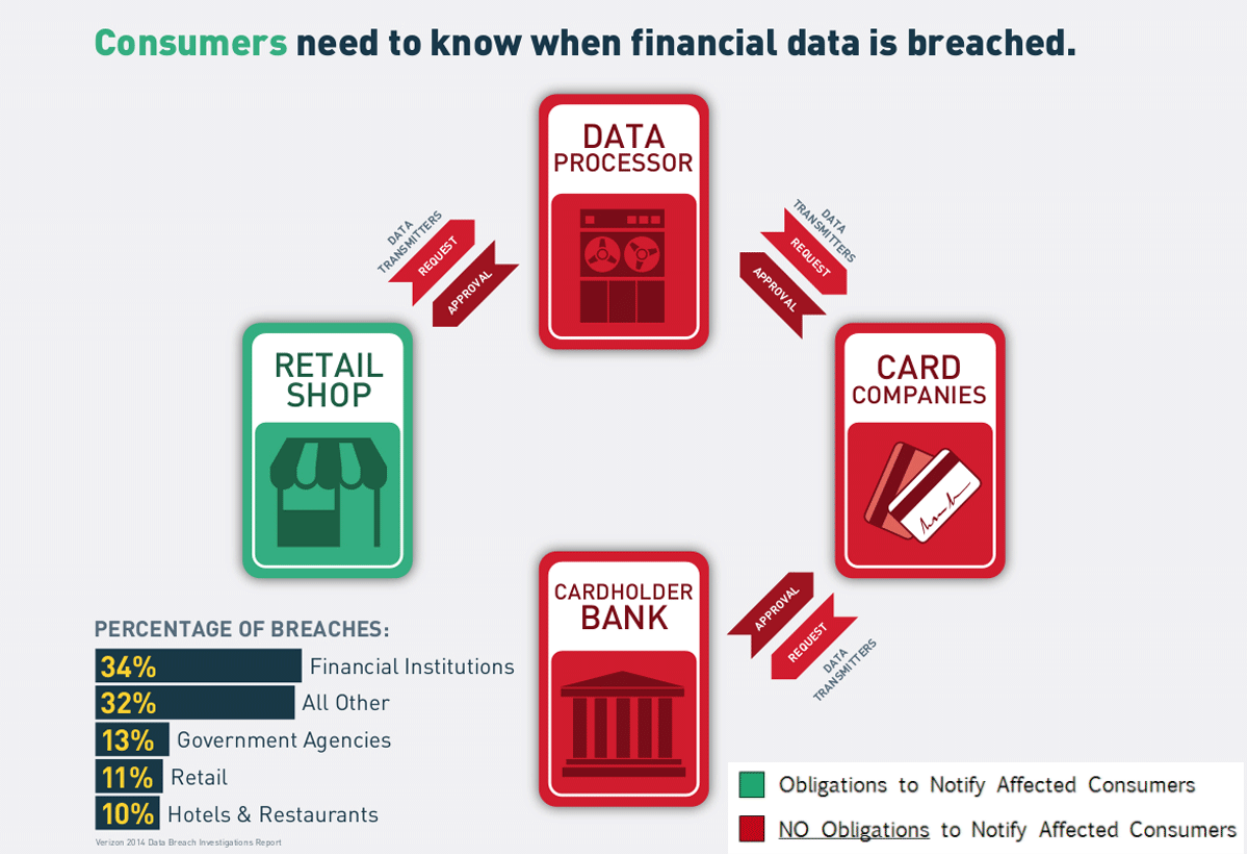
Given the breadth of these invasions, if Americans are to be adequately protected and informed, federal legislation to address these threats must cover all of the types of entities that handle sensitive personal information. Exemptions for particular industry sectors not only ignore the scope of the 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 Entities – Insufficient Notice Rule in Section 3(b) of Discussion Draft

Figure 2, below, illustrates how section 3(b)(1) of the discussion draft would operate with respect to notice by "third-party entities" operating in the payment system. This graphic illustrates a typical payment card transaction in which the Energy and Commerce 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 to provide greater clarity of the general payment flows.) Section 3(b)(1) of the discussion draft would only require the retail shop, in this example, to provide consumer 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 the discussion draft's definition of "covered entity" in section 5. Comparing this to figure 1, this consumer notice regime presents an inaccurate picture of the breadth of breaches to consumers. Furthermore, such a notice regime 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 public disclosure burden for every other entity in the networked system that suffers a breach, then 100% of the notices would come from the 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 the important point about the risks of over-notifying and confusing American consumers if this proposed third-party notice rule illustrated in *Figure 2* is adopted by the Subcommittee. The largest payment card breach in history occurred at a payment processor, Heartland Payment Systems, which was breached in 2008 and resulted in the compromise of over 130 million payment cards. If Heartland had to follow the proposed third-party notice rule in the discussion draft, 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 had 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.

One consequence of this circuitous disclosure process is that it could ultimately lead to over-notification and confusion of consumers about the payment processor's breach that may affect them. For example, if affected consumers shopped at a number of retailers that all used the same payment processor that suffered the breach (e.g., Heartland, in this hypothetical), the consumers could potentially receive slightly different notices from each store – all providing an account based on what they knew about the breach by the same payment processor – when none of those branded retail stores actually suffered the breach itself. This third-party notice structure would create an untenable public policy "solution" that neither serves consumers nor the multiple non-breached businesses that are providing notice for the breached one.

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 should go further than the proposed third-party entity provision in section 3(b) of the discussion draft: it should 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 publicly reporting known breaches of their own systems. If we want meaningful incentives to increase security, everyone needs to have skin in the game.

Service Providers – Exemptions from Providing Any Notice under Section 3(e)

Another – and even wider – notice hole that has remained unplugged for many years in other legislative proposals, and remains as a holdover in this discussion draft, is the exemption permitting service providers to avoid notification of their breaches altogether, even when aware of them. Section 3(e) of the discussion draft 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 if it fails to identify them.

Other businesses, such as retailers, however, would be required by the discussion draft to provide notice even if the breached entity does not have the contact information for affected consumers, which is often the case for a retailer when payment cards are breached. In those instances, other covered entities must provide substitute notification. Why not service providers?

The service provider exemption in section 3(e) is drafted so as to permit no notice at all to be made, not even to the FTC or other federal 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 engineered such an exemption in past legislative proposals that had no prospect of passing Congress.

Allowing this type of notice hole in legislation that this Subcommittee would proffer as a "uniform" breach notification bill makes no sense. Just because a telecommunications provider or another company qualifying as a "service provider" may provide a service to another business does not mean it should be permitted to escape providing notice of its data breaches. With an exemption for service providers like the one contained in section 3(e) of the discussion draft, there would be a real risk that the public would not learn of the providers' breaches in most instances and consumers would not get the information about the breach they need to potentially protect themselves.

Furthermore, under the discussion draft, if a service provider can identify the sender of a transmission that was affected by a breach, it must notify the sender, but then has no further obligations under the bill. This means that, even where it can identify an affected customer, other businesses will have to plug this notice hole and take the attendant cost and blame for providing consumer notice of the service provider's data breach. The legal liability can be severe, for example, if the service provider does not provide information in a timely fashion such that the non-breached company with the notice obligation cannot make timely notice within 30 days.

The discussion draft's section 3(e), therefore, amounts to both a *notice-shift* and a *liability-shift* by the breached service provider onto their clients who were not breached but were victimized by using the breached service provider. It begs the question as to what findings the committee has made, and what evidence does it have in the record, to justify this kind of provision, which has no precedent in any of the 47 state breach notification laws. In fact, inclusion of such a provision in a preemptive bill would mean a reduction in disclosure requirements for service providers (as defined in this discussion draft) form the obligations they currently have under state breach notification laws today.

Finally, as noted above, such a notice hole for service providers reduces their incentives to improve their data security systems and protect customer data because it leaves them with no skin in the game even when they suffer a breach of security in their provision of services.

Financial Institution Exemptions – Definition of "Covered Entity" in Section 5

Many legislative proposals last Congress had notice holes, such as those noted above, where consumers would not receive disclosures of breaches by certain entities. Perhaps the notice hole that has been left unplugged in most proposals, and again is left wide open by the discussion draft's definition of "covered entity" in section 5, is the exemption for financial institutions. We understand and appreciate the *jurisdictional* limitations of the Energy and Commerce Committee at this stage in the process, but it is worth pointing out for the record that the discussion draft's exempted entities – those subject to the Gramm Leach Bliley Act (GLBA) – do not have any federal statutory language that requires them 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 effectively address this lack of a federal notice requirement when it set forth an essentially precatory standard for providing consumer notice in the event that financial institutions 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] The existing guidelines for financial institutions fall far short of creating a federal notification "requirement" that the Subcommittee would impose on all other entities by using the language of "shall" – an imperative command used in the discussion draft's section 3 notification rules (i.e., *see* p. 3, line 1, third word) 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.

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 always 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 the discussion draft, despite the fact that financial institutions hold Americans' most sensitive financial information. By comparison, a number of the more seasoned and robust state laws, such as California's first-in-the-nation breach notification law, have not exempted financial institutions from the state 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 affecting them.

[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.

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

Conclusion –Proposed General Principle for Effective Notice by All Breached Entities

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 adopt notification standards that "follow the data" and apply to any entity in a networked system 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. Furthermore, for most payment card breaches, the entity closest to the affected customers – the entity that has the affected customers' contact information because it bills them monthly – is the card-issuing bank that the proposed discussion draft exempts and that the FTC has no jurisdiction over. This is yet another notice hole that applies to the theory of "closest-to-the-consumer" notice in many cases.

This is not to say, however, that a notice provision is impossible to construct that would address the concerns above. In fact, in our discussions with state attorneys general about the deficiencies of the third-party entity notice obligation in their state's laws, it became apparent that the guiding principle should be "effective" notice, of which relationship to the customer is only one fact, and other considerations such as the speed, uniformity and clarity of the consumer notification must also be taken into account. In the Heartland example above, for instance, the payment processor made substitute notice because that was the most effective way to notify 130 million card holders. It did not follow the deficient third-party entity rule in this discussion draft, and this Subcommittee should not force companies to make ineffective customer notice either.

Indeed, a public notice obligation on all entities handling sensitive data would require consumer notification whenever and wherever a breach occurs. In doing so, it 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.

Legislation Should Establish a Nationwide, Uniform Standard Preemptive of State Law

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 (e.g., the District of Columbia, Guam, Puerto Rico and the Virgin Islands) have enacted varying data breach notification laws.[4] 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, provisions 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, which are subject to all of the state and federal territory breach disclosure laws, have met the burden of providing consumer notice, even when they did not initially have sufficient information to notify affected individuals, through the standardized substitute notification procedures in each state law. However, with an increasingly unwieldy and conflicting patchwork of disclosure laws covering more than fifty U.S. jurisdictions, it is time for Congress to acknowledge that the experimentation in legislation that exists at the state level and that defines our federalist system has reached its breaking point, and it is time for Congress to step in to create a national, uniform standard for electronic data in interstate commerce in order to ensure uniformity of a federal act's standards and 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 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.

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 stakeholders in breach notice legislation, like NRF, have called for a more robust notification standard at the federal level than currently 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" noted above, thereby establishing a breach notification standard that applies to all businesses – a comprehensive approach the Energy and Commerce Committee and this Subcommittee have adopted in previous consumer

[4] *See,* National Conference of State Legislatures (NCSL) website for a complete list of the 51 jurisdictions with breach notice laws, and 3 states without a breach law: http://www.ncsl.org/research/telecommunications-and-information-technology/security-breach-notification-laws.aspx

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.

Unclear Effect of Preemption Language in Section 6 of Discussion Draft

The discussion draft's section 6 includes a clause intending to preempt the application of state breach laws, but it couples it with a not-yet-finalized, bracketed clause that would preserve a covered entity's "liability under common law." Despite the inclusion of language in the bill's enforcement section that private causes of action cannot be brought against covered entities for "a violation of this Act," inclusion of the preemption clause language preserving common law liability would mean that retailers who are in full compliance with this act's provisions would remain potentially liable under various common law claims by singular or class action plaintiffs.

Furthermore, the federal courts have ruled that a carve-out for some state laws in preemption clauses creates sufficient ambiguity as to Congressional intent as to jeopardize the entire preemption clause (see, e.g., CAN-SPAM Act of 2003). We have urged members' staff in our previous discussions not to construct a preemption clause in a form that may lead to greater uncertainty in the language and, therefore, potential legal challenges to the preemptive effect of the federal law in the 51 jurisdictions where breach laws have been enacted.

Preemption of state laws and common laws that create differing standards of care 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 may not result in the preemption of related state laws. In fact, attempts to limit preemption may only result in adding yet another law, this time a federal one, to the panoply of 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.

Data Security Standards for General Applicability to Businesses

Collectively, retailers spend billions of dollars safeguarding sensitive customer information and fighting fraud. Maintaining the trust of retail customers by preventing the theft of sensitive personal information related to retail shopping, and the potential fraudulent use of that data by criminals, is at the top of our industry's priorities. It should not be surprising, then, that data security is something in which our members invest heavily and strive to improve every day.

The Subcommittee should keep in mind, though, that security is like defense, and while a retailer could theoretically spend all of its money on defense, it would still not be 100% protected from all attacks. As it is with our national defense and the protection of government facilities alike, the reality of corporate data security is that it is much more difficult to implement than what is theoretically possible, especially if it must be robust enough to defend against attacks like those perpetrated against every sector of American industry from foreign-based criminal organizations that, as we have seen, may be directed, facilitated or tolerated by the host nation states from which they operate and launch their malicious cybersecurity attacks on U.S. corporate networks.

Federal and State Data Security Standards Apply to All Retailers

The Federal Trade Commission (FTC) has often recognized, including in its testimony before Congressional committees, the reality that businesses implementing data security safeguards should not be expected by government to be 100% protective – that is, capable of successfully defending against every attack every time. As a result, the FTC has effectively determined that businesses should be held to "reasonable" data security standards and that the fact of suffering a breach, alone, is not sufficient to determine whether or not a business met this standard. Once again, beyond the theoretical, the reality is that the FTC vigorously enforces a reasonable data security standard against all businesses subject to its jurisdiction.

The FTC has already brought over 50 actions against companies nationwide in a range of industry sectors for what it claims are unreasonable data security practices. The Commission exercises this authority under Section 5 of the FTC Act (15 USC 45), which prohibits "unfair or deceptive acts or practices in or affecting commerce" – a prohibition that applies to all entities engaged in commerce. When the Commission believes a business has fallen short in providing reasonable data security protections for sensitive personal information, it typically (but not exclusively) acts under the "unfairness" prong of Section 5, finding a business in violation where its data security practices cause, or are likely to cause, substantial injury to consumers that cannot be reasonably avoided by those consumers and are not outweighed by countervailing benefits to those consumers or to competition.

This, by definition, is a subjective determination made by the FTC, and not a set of static requirements. Because of this, the FTC's authority under Section 5 is limited to bringing entities under a cease and desist order for potential violations, and not fining them for data security practices with which they may otherwise not recognize are "unfair" in the eyes of the Commission enforcement attorneys. Nonetheless, rather than face an administratively determined cease and desist order, 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.

Our members recognize the severity of this federally-imposed data security standard enforced by the FTC under Section 5 of the FTC Act, which applies to all businesses subject to the FTC's jurisdiction. Additionally retailers are subject to and comply with a range of state

laws specifically governing data security, as well as state consumer protection regulations enforced through their consumer protection agencies and/or their attorneys general. This robust set of existing law, enforced aggressively by the FTC and subject to enforcement by a range of state AGs for data security failures, is a reality, even though some in the financial services community attempt to perpetuate the myth that retailers are not subject to any data security standards under the law.

Payment Card Industry Data Security Standards Apply to All Retailers Accepting Cards

In addition to the federal and state laws, any merchant that accepts bank-issued credit or debit cards from consumers must comply with more than 220 specific data security requirements dictated by the card industry's Payment Card Industry (PCI) Data Security Council. These data security standards, enforced by rules and contract, present another tier of liability and significant annual expense for merchants on top of federal and state government actions. Under the PCI data security standards, card-accepting merchants must protect payment card transactions and submit annually, at considerable cost, to certification processes.

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 – effectively control the PCI Data Security Council that is responsible for setting the PCI data security standards for payment cards. Unlike other technical standards-setting bodies that are comprised of stakeholders from those industries that have an interest in, and/or will be subject to, the standards, PCI standards are imposed by the payment card industry on all card-accepting businesses across a variety of industries without providing card-accepting businesses any real vote in the standards processes imposed upon them, relegating merchants to near meaningless "advisory" positions, at best. Nevertheless, 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.[5]

Effect of Imposing GLBA-Like Standards on Businesses Subject to FTC Enforcement

Despite this robust, multi-tiered data security standards and enforcement regime, which includes federal, state and banking industry-imposed data security standards, some in the financial services community attempt to perpetuate the myth that other businesses, including retailers, are not subject to any general data security standards or specific requirements, apparently overlooking the requirements that branded payment networks themselves have already imposed on card-accepting businesses through the PCI Data Security Council that they exclusively control. The members of this Subcommittee should recognize the truth about data security standards borne by card-accepting businesses as it examines this issue, and whether it is necessary and appropriate to impose an additional GLBA-like federal data security standard on top of the existing standards under which these businesses, including retailers, are already complying nationwide.

[5] The card networks have made those decisions *for* merchants, not *with* merchants, and the increases in fraud demonstrate that *their* decisions have not been as effective as they should have been. In fact, it reflects the reality that specific, operational data security standards are often a generation behind the criminals that invest heavily in developing new methods to defeat what they know to be the industry-prescribed standards.

As a result of the little-understood differences in the data security standards and enforcement regimes faced by banks under the banking regulators versus the standards faced by the wide array of businesses (including retailers) subject to FTC enforcement, not to mention the substantive and well-considered reasons behind those differences in standards and enforcement, we sought an expert opinion on the effect of applying a GLBA-like data security standard to non-financial businesses. Specifically, we asked for an analysis of whether it would be appropriate and effective for proposed federal legislation to impose banking industry based data security standards on the full array of commercial businesses, ranging from large multinational conglomerates to small operations, that are not "financial institutions," including every non-banking business in America that accepts virtually any form of tender other than cash (e.g., credit cards, debit cards, checks, etc.) from customers in exchange for goods and services.

As part of your efforts to craft data breach legislation, we strongly encourage you to review the white paper attached as *Appendix A* to this testimony, which was just released by two former associate directors responsible for financial and credit practices in the FTC's Bureau of Consumer Protection. As the excerpts from the white paper below demonstrate, this analysis provides a valuable perspective to the Subcommittee and indicates why we believe the broad expansion of data security standards similar to the GLBA guidelines to virtually every unregulated business in the U.S. economy would be a serious error.

• **Would Cover Virtually All Providers of Consumer Goods and Services:** As noted in the executive summary of the white paper, the authors demonstrate the broad impact from FTC enforcement of GLBA-like data security standards:

> *"Because of the near-universal acceptance of bank-issued cards as payment for goods and services, companies that would be subject to the Guidelines' standards would include merchants, hotels, bars and restaurants, theaters, auto dealers, gas stations, grocery and convenience stores, fast-food eateries, airlines and others in the travel industry, hospitals and doctors, dentists, veterinarians, hair salons, gyms, dry cleaners, plumbers and taxi drivers. In other words, <u>virtually all providers of consumer goods and services</u> would be covered." (emphasis added)*

• **Safeguards Designed for Banks are "Poor Fit" for Card-Accepting Businesses:** As the white paper's analysis explains in greater detail, financial institutions have multi-factored requirements for data security because they routinely have much broader sets of the most sensitive personal and financial customer information in digitized form, which presents security risks and vulnerabilities not evident in most unregulated commercial businesses with much narrower data sets with less sensitive customer information. The authors explain several reasons why data security "safeguards requirements designed for closely supervised banks that issue credit and debit cards are a poor fit for the vast array of entities that accept credit cards and debit cards as payment for their goods and services." For example:

> • **Banking Examination is Interactive Guidance Process; No Comparable Guidance for Vast Array of Businesses under FTC Adversarial Process:** GLBA guidelines are "premised on an ongoing and interactive process between regulator and

regulated entity, whereby examiners can instruct a bank on an apparent failure to meet a specific requirement. This process enables the institution to explain why a particular element of the Guidelines may be inapplicable or to correct any real deficiencies without legal sanctions." The vast array of businesses subject to FTC jurisdiction have no comparable process. Rather, "the FTC obtains compliance by initiating law enforcement investigations, using compulsory process, when it suspects a potential law violation based on facts that have come to its attention." The FTC's "after the fact" adversarial review process may lead to fines imposed on a business for noncompliance of which it may not be aware until it is under investigation by the FTC.

• **Card-Issuers Have Capabilities to Control Card Security; Card-Accepting Businesses Have Least Ability to Ensure Card Security:** The obligations on card-issuing banks under the GLBA guidelines are "premised on the specific circumstances and capabilities of card **issuers**, which differ substantially from those of entities that accept cards as payment." It is the banks that dictate to the card-accepting merchants "the card processing capabilities of the equipment and procedures that merchants must use, as well as the security features inherent in the cards." Furthermore, the authors conclude that: "Were the FTC required to enforce safeguard standards for credit and debit card data based on the Guidelines' model, it would be imposing obligations on the entities with the least ability to ensure that they were carried out." In essence, card-accepting businesses do not control the security features of the cards themselves; that is what banks control and one reason why they are subject to GLBA guidelines whereas the FTC made the determination that it is not appropriate to apply the same guidelines to businesses that simply accept payment cards.

• **Would Not Enhance Consumer Protection:** The executive summary concludes by noting that the FTC had previously applying such a rule:

> *"Subjecting nonbank businesses to the Guidelines' specific requirements would not enhance the FTC's ability to use its existing authority to protect consumers through enforcement actions. When it issued consumer information privacy and safeguards rules under the Gramm-Leach-Bliley Act, the FTC considered applying the rules to retailers that accept bank credit or debit cards and declined to do so. We believe that determination remains equally justified today." (emphasis added)*

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 fined by their regulators for data security weaknesses. But, as noted above, commercial companies paid huge settlement penalties to the FTC. Providing an agency like the FTC, tasked with an adversarial and investigative *enforcement* approach, a set of standards with significant room for interpretation is likely to lead to comparatively 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 Congress that no system – even the most protected one money can buy – is ever 100% secure.

Comments on Data Security Section of Discussion Draft Legislation (Section 2)

In light of the Subcommittee's expedited schedule, we have preliminarily reviewed section 2 of the discussion draft, which provides requirements for information security. The comments below reflect our *initial* views on the draft language of this section:

1. Section 2 Could Expand FTC Enforcement Authority Beyond Existing Reasonable Data Security Standard as the General Rule for All Businesses

While the discussion draft's language is not identical to GLBA data security guidelines, we are concerned that it could be interpreted by the 50 state attorneys general as an expansion of FTC authority in the area of data security enforcement. We understand that other stakeholders may view the following words at the end of the section – "as appropriate for the size and complexity of such covered entity and the nature and scope of its activities" (emphasis added) – as an intended limiting feature to the reasonableness test, but those words could have a different effect in practice. As drafted, these words are in addition to the reasonable standard provided earlier in the section and could create in federal law an additional four-factor test for what constitutes reasonable data security that would go beyond a general standard of "reasonableness" whether cabined in under the unfairness prong or free standing under Section 5 of the FTC Act. This multi-factored test could exponentially increase the risk of a breached company being found at fault by the FTC for a breach, even if the company's data security would have survived an overall reasonableness test under Section 5 of the FTC Act as it is enforced by the FTC today.

For example, this section could be interpreted to mean that the FTC may only have to believe that a company was unreasonable as to any one of the four factors specified in section 2 in order to claim a potential violation of the FTC Act, rather than needing to show that the company had an overall unreasonable data security program. If interpreted in that fashion, it would present an exponentially greater risk because, with four factors, there are 15 ways the FTC could determine a company's program fails this test, and only 1 way a company passes it: that is, if all 4 factors, as applied to its data security program, are independently "reasonable."

We note that the section 2's information security standard would apply to every type of data that falls within the definition of "personal information" in section 5 of the discussion draft. This means that names, addresses, and birthdates (a combination that is often found in marketing lists and that, alone, generally cannot lead to identify theft) and other typically non-sensitive information must be protected along with more sensitive information such as Social Security Numbers, which could be used to perpetrate fraud and identity theft. This leads to a potentially broader, complex and expensive data security regime for all businesses to implement.

But how does the owner of a chain of dry cleaners, a hair stylist, a veterinarian or a small shopkeeper determine if their data security protection for either payment cards or customer information is reasonable as to the factor of the "size" and "complexity" of its business? Will they understand what that means either directly or in relation to other businesses of their type?

How will they know if they are reasonable as to the "nature" and "scope" of their business activities in the eyes of the FTC? Must these and the vast array of American businesses engage in some kind of comparative analysis between the "size" of other companies or as to the "nature" of their customer information practices – and what does that comparative analysis look like, and what will it cost to obtain? Will every Main Street storefront and service provider in the U.S. now incur costs to hire lawyers in Washington, with specialized FTC practices, simply to ensure that the off-the-shelf equipment and systems for either customer relationship management (CRM) or payment card acceptance will survive an FTC multi-factor reasonableness test? Can they afford not to take this step if the FTC could fine them for non-compliance? And will this require a constant reinvestment in new equipment and/or in new software every single time a more sophisticated attack is discovered that will defeat that technology?

Questions such as the ones above do not come with easy answers, and we do not have them after the limited period of review we have had with this language. However, before the Subcommittee marks up legislation that may add a new information security standard applicable to a vast array of American businesses, we urge it to examine not only the intent of the words it would include in the legislation, but the potential ways such words could be interpreted by the courts, who will turn to the words of the statute itself in applying the law.

Lastly, the FTC's "reasonable" data security standard enforced today may already take into account the four factors in section 2 above, since those factors are not found in the FTC Act itself. If so, there may be an argument that could be made that there is no need for inclusion of the factors now. Indeed, nearly all state breach laws, including California's first-in-the-nation breach notification law, that have added a data security standard over the years have used only the word "reasonable" in the statutory text without reference to additional factors. We recommend that the Subcommittee closely examine the data security standards in existing state breach laws and consider the points above before instituting a new, multi-factor test of reasonableness in federal law for broad application to a wide range of commercial businesses.

2. Section 2 Factors Appear to Apply "Guidance Standards" in an FTC Enforcement Regime that is Not Designed to Offer Interactive Guidance to Businesses

Because the FTC is an enforcement agency without the capability, staff or funding to provide supervisory guidance to all businesses under its jurisdiction, even the most sophisticated nationwide businesses that are tasked with designing data security programs in compliance with this new standard would not necessarily know whether and when they would potentially fall out of compliance with the standard before coming under investigation by the FTC.

As noted above in the discussion of the white paper attached as *Appendix A*, unlike the bank examination process where banks engage in an iterative and interactive process with bank examiners to develop a data security program appropriately tailored to the size and complexity of its business and the nature and scope of its information practices in compliance with the GLBA guidance standards, there are no such examiners at the FTC to provide "before-a-breach" guidance on what aspects of a business's data security program are, or are not, in compliance with the discussion draft's multi-factor standard that could be enshrined in federal law and enforced with civil penalties imposed by the FTC and state attorneys general.

Since it is unlikely that this Congress would approve a sharp increase in the size of the FTC's staff – perhaps by tens of thousands of examiners – to provide bank-like supervision and guidance to every business in America, this Subcommittee, which has oversight responsibility for the FTC, should consider the potential impact of imposing guidance-like language, similar to GLBA, on every non-financial business in America under an FTC enforcement regime run by an agency that is incapable of providing the basic guidance and interactive process necessary to ensure businesses have an opportunity to be in compliance with these standards.

3. Section 4 Would Grant the FTC Authority to Fine Any Businesses it Deems in Non-Compliance Before the Business Could Even Know It Is Out of Compliance

As noted above, companies have no opportunity to obtain supervisory guidance from the FTC to ensure they are in compliance with what the FTC (in its own discretion) determines is "reasonable" information security under the four-factor test of section 2. Nevertheless, even without the chance of knowing that they may be out of compliance until they come under an FTC investigation, these companies would still face the prospect that the FTC can immediately impose civil penalties on them for claimed violations of section 2 because this provision would be enforced under the trade regulation rules in section 4 of the discussion draft (e.g., "a regulation under Section 18(a)(1)(B) of the Federal Trade Commission Act (15 U.S.C. 57a(a)(1)(B))").

Unlike the FTC's existing authority under the FTC Act's Section 5 today, the bill would not require the FTC to first bring a company under a cease-and-desist order for noncompliance before it could go straight to imposing fines on it for violations of the Act. This type of civil penalty authority under the trade regulation rules is more justified for enforcement of clear disclosure requirements where the threat of government fines serves as a deterrent to bad actors shunning the law (i.e., the reason why it was authorized in the CAN-SPAM Act of 2003).

Unlike regulated banks who work with examiners to get a data security program right, companies subject to FTC enforcement under section 4 would have no way to determine if they are passing the section 2 test for reasonable data security before being subject to potentially millions of dollars in government-imposed fines. We recommend the Subcommittee reconsider the application of trade regulation rule enforcement to section 2's subjective data security standard, and consider maintaining the same enforcement authority the FTC has today under Section 5 of the FTC Act for unfair or deceptive acts or practices.

4. Consequences of Potential Expansion of FTC Enforcement Authority

Pulling together the potential consequences of the discussion draft's section 2 information security standard and section 4's enforcement standard that are raised in the more detailed comments above, the proposed provision would appear to an expansion of the FTC's existing enforcement authority and a potential extension of the reasonable data security standard it currently enforces into a GLBA-like multi-factor guidance test to apply to all non-financial

companies.[6] It is important to note that, as coupled with section 4's enforcement language, this standard would be enforced against these companies in a much more severe way than GLBA is enforced against financial institutions. What is being proposed in the discussion draft may therefore be considered to be beyond any rule the banks have in terms of enforcement for programs designed to protect and secure the most sensitive personal and financial information.

Congress should be cautious in weighing in on the question of FTC authority when the agency has pending litigation on the extent of that authority. This is especially important given a government enforcement agency's natural inclination to rush in to determine "who killed the cat" whenever there is a "dead cat" on the floor (i.e., in this instance, when a data breach has occurred). Following breaches, the victim of a crime that had in place reasonable data security practices prior to the breach may, nonetheless, be accused of malfeasance when the organized criminal organization that perpetrated the crime cannot be identified or prosecuted.

Congress should recognize that these criminals have developed and used technology to breach networked systems that is often superior to the state-of the-art data security technology available to U.S. companies from security vendors. As a result, the Subcommittee ought to be wary of attempts to codify new, statutorily-based and subjectively-determined data security rules (that would be enshrined in the federal law separate and apart from the "unfairness prong" of Section 5 of the FTC Act) to apply to all business in America where: (i) these businesses are not engaged in financial services, as previously determined by the FTC; (ii) the FTC cannot provide bank-like supervisory guidance as to how a business's specific program may come into compliance with the law; and (iii) the subjective standard would be enforced with government fines (not just cease-and-desist orders) against businesses who cannot know in advance if they are in compliance or not.

Conclusion Regarding Generally Applicable Data Security Standards in Legislation

As noted above, NRF and its members support data security standards, and if a standard is to be included in federal breach legislation, it needs to be a general standard that is appropriate to the broad array of businesses it would cover (similar to FTC Act Section 5's prohibitions on "unfair or deceptive acts or practices") and, because it is general, must be enforced consistent with the Commission's long-standing practices under Section 5.

[6] For those who point out that it is <u>not</u> GLBA, we agree that the proposed discussion draft section 2 provision is not identical to the data security guidelines that apply to financial institutions, but nor should it be, given the significant differences between the most sensitive customer information and complex financial data sets held by financial institutions, a combination with unique vulnerabilities and risks that do not apply to most every other business in America. But section 2, especially when subject to FTC enforcement and civil penalty authority, is also not a lower standard or "GLB-lite," as some have suggested, because banks would not be subject to the imposition of fines for a first violation of subjective standards section 2 would impose. Section 2 would, in fact, apply a stricter enforcement regime on every business in the U.S. for the protection and security of information that is typically much less sensitive than the information banks themselves hold. As Congress should recognize, the imposition of higher standards and more severe penalties for the protection of less sensitive information is not one of the "Fair Information Practice Principles."

Proper Scope of Breach Law – Definition of "Personal Information" in Discussion Draft

In general, the draft bill requires "personal information" (or "PI") to be protected and secured against "unauthorized access," and if any PI is accessed or acquired in a breach of security, public notification may be required depending on the type of entity suffering the data breach (as noted above). Notably, the bill contains an expanded definition of PI that is much broader than the PI definitions in most state laws. For example, the combination of a customer's name, address and birthdate is now considered to be PI. Similarly, a "unique account identifier," such as one used for CRM purposes, is also considered PI.

This expansive definition of PI could, if enacted as drafted, impact a business's operation while not providing any corresponding benefit to consumers either from breach notification or increased security of certain types of PI included in the discussion draft's definition. Additionally, the inclusion of some types of information in the definition of PI may have the unintended consequence of discouraging security steps that businesses might otherwise take to minimize sensitive data in their systems through use of non-sensitive "unique account identifiers." Several examples of problematic data elements in the PI definition are as follows:

- **Name+Address+Birthdate or Name+Phone+Birthdate:** The definition's inclusion of a combination of a name, address/phone and birthdate is overly broad and portends to sweep in a significant amount of marketing or CRM data that, if breached, would not (alone) lead to identity theft. This combination of information, for example, might be used by retailers and restaurants for promotional reasons (e.g., providing a discounted gift or dinner on your birthday) or to narrow offerings to certain eligible groups (e.g., catalog or promotion for seniors) In fact, it is hard to determine the intended purpose of breach notification for this combination of information – without other information also being breached – if no harm is reasonably likely to result from it and if there is nothing further a consumer might do to protect himself or herself once notified that a marketing list with this information was lost. These may be some of the reasons why most state breach notice laws <u>do not</u> include this combination in their definitions of covered data for breach notification purposes. Additionally, because the bill requires all PI to be protected with information security, inclusion of this combination of non-sensitive "phone book" or market segmentation information will need to be as protected as the most sensitive information, such as Social Security Numbers maintained by a business in its HR/employee records. The increased cost to secure benign marketing data may be absorbed by reductions in the amount of promotions offered to consumers even though there is no concomitant benefit to consumers from the additional security required under the bill. Lastly, we note that the definition of PI excludes information that is derived from public sources, and yet the combinations of "phone book" data in this section could exclusively come from public sources in most cases, raising additional questions as to the necessity of these combinations in the definition of PI.

- **Unique Account Identifiers:** The PI definition would also include a "unique account identifier…in combination with any associated security code [etc.]…that is required for an individual to obtain money, or purchase goods, services, or any other

thing of value." This is an extraordinarily broad element of PI that could possibly include a shopper's phone number (a unique account identifier) entered into a numeric pad on a store's point-of-sale system to obtain a discount (based on a loyalty program) in connection with a store purchase. We are not aware of any state breach law that would include as PI a stand-alone phone number, and yet in this scenario, one might be covered by this discussion draft's definition and require notification if breached. Additionally, as retailers strive to minimize data by replacing sensitive data with tokens (unique account identifiers), inclusion of what has traditionally been seen as non-PI unique identifiers in the definition may discourage companies from making the investment to de-identify or minimize sensitive data if it will still be subject to the same data security standards and lead to notification following a breach, even if that unique account identifier could not directly be used (alone, and without more associated sensitive information tied to it that is also breached with it) to identify or harm an individual. If the discussion draft is to continue to have unique account identifiers in the definition, then to address the concerns above, we would recommend it be qualified, at a minimum, by requiring that such identifiers are only PI if they could "alone be used to gain access to an individual's account" for the purposes of obtaining money or purchasing goods or services.

Improving Technology Solutions to Better Protect Consumers in Payment Transactions

Improving Payment Card Security

On October 17, 2014, the President signed an executive order initiating the BuySecure Initiative for government payment cards.[7] 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 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.

An overhaul of the fraud-prone cards that are currently used in the U.S. market is long overdue. 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 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.

[7] 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

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."[8]

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.[9] 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 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.

[8] The Nilson Report, Issue 934, Sept. 2009 at 7.
[9] 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.

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."[10] 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 federal legislation, in line with our principles, that would standardize and streamline the breach notification process so that consumers may be treated equally across the nation when it comes to the disclosure of data security breaches affecting them, NRF also supports a range of legislative solutions that we believe would help improve the protection of debit card holders, the security of our networked systems, and the law enforcement tools that could be employed to address criminal intrusions,.

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

From the perspective of many consumers, one type of payment cards has often been as good as another. Consumers, however, 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 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.

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

Legislation Protecting Businesses that Voluntarily Share Cyber-Threat Information

NRF also supports the passage by Congress of cybersecurity information-sharing legislation like H.R. 624, the "Cyber Intelligence Sharing and Protection Act," cosponsored last Congress by Congressmen Rogers and Ruppersberger, which passed the House with bipartisan support. Legislation like this would protect and create incentives for private entities in the commercial sector to lawfully share information about cyber-threats with other private entities, and with the federal government, in real-time. This could 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. **Require Public Notice for All Businesses Handling Sensitive Data**: 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. **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.

3. **Establish Uniform Nationwide Standard through 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.

Appendix A:

White Paper on Data Security Standards

(See separate attachment)

The Effect of Applying Customer Information Safeguard Requirements for Banks to Nonfinancial Institutions

Joel Winston and Anne Fortney
March 2015

We have been asked to analyze the effect of legislation requiring the Federal Trade Commission ("FTC") to apply standards based upon the Interagency Guidelines for banks in Safeguarding Customer Information ("Interagency Guidelines" or "Guidelines") to any entity that accepts bank-issued payment cards for goods and services and does not extend credit itself.

Summary

The Interagency Guidelines for Safeguarding Customer Information apply to depository institutions ("banks") subject to supervisory examination and oversight by their respective regulatory agencies. The Guidelines contain detailed elements of an information safeguards program tailored specifically to banks. They are designed to be a point of reference in an interactive process between the banks and their examiners, with emphasis on compliance on an on-going basis. The FTC has issued a Safeguards Rule applicable to the nonbank "financial institutions" under its jurisdiction. The Safeguards Rule provides for more flexibility and less specificity in its provisions than do the Guidelines. The more general requirements of the FTC's Rule are designed to be adaptable to ever-changing security threats and to technologies designed to meet those threats.

The differences in the approaches to data security regulation between the Guidelines and the FTC Safeguards Rule reflect two fundamental differences between the bank regulatory agencies (the "Agencies") and the FTC: the substantial differences in the types and sizes of entities within the jurisdiction of the Agencies versus the FTC, and the equally substantial differences in the roles played by the Agencies and the FTC in governing the behavior of those entities. With respect to the former, while the banks covered by the Guidelines are relatively homogeneous, extending the Guidelines to all entities that accept payment cards would sweep in a vast array of businesses ranging from large multinational conglomerates to small operations, and could also include individuals.[1] The threats faced by these widely diverse businesses are likely to vary widely as well, as would the sophistication and capabilities of the entities themselves for addressing the threats. A flexible approach as in the Safeguards Rule is necessary to account for those critical differences. Many of the Guidelines' provisions, which were drafted with banks in mind, likely would be unsuitable for a significant proportion of the entities that would be subject to these new requirements.

[1] Because of the near-universal acceptance of bank-issued cards as payment for goods and services, companies that would be subject to the Guidelines' standards would include merchants, hotels, bars and restaurants, theaters, auto dealers, gas stations, grocery and convenience stores, fast-food eateries, airlines and others in the travel industry, hospitals and doctors, dentists, veterinarians, hair salons, gyms, dry cleaners, plumbers and taxi drivers. In other words, virtually all providers of consumer goods and services would be covered.

For similar reasons, the different approaches the Agencies and the FTC take in regulating their entities make it problematic to apply the Guidelines to the nonbank entities overseen by the FTC. The more specific Guidelines make sense when, as is the case with the banks, there is an ongoing, interactive dialogue between the regulated entities and the regulator through the supervision process. The regulated entities and regulators can address changes in threats and technologies during the less formal examination process and head-off potential problems before they happen. By contrast, the Safeguards Rule's flexible requirements are better suited to a law enforcement agency like the FTC that obtains compliance not by an interactive dialogue, but by prosecuting violations after-the-fact. Indeed, an entity within the FTC's jurisdiction may have no indication of deficiencies in its compliance until it is under investigation. With the untold numbers of entities potentially subject to its jurisdiction, the FTC simply lacks the capability or resources to engage in dialogue or provide the individualized, ongoing guidance like the Agencies do with their banks.

While the Guidelines would be made applicable to any entity that accepts bank-issued payment cards,[2] the Guidelines' specific requirements are suitable only for the bank card-issuers that dictate the card processing equipment and procedures for businesses that accept their cards, as well as the security features inherent in the cards. If the Guidelines were made applicable to businesses that merely accept banks' cards, they would impose security obligations on those with the least ability to implement the requirements applicable to payment card security.

Finally, nonbank businesses are subject to the FTC's general authority under the FTC Act to prohibit unfair or deceptive practices, and the FTC has prosecuted many companies under this authority for failing to protect consumer's nonpublic information. Subjecting nonbank businesses to the Guidelines' specific requirements would not enhance the FTC's ability to use its existing authority to protect consumers through enforcement actions. When it issued consumer information privacy and safeguards rules under the Gramm-Leach-Bliley Act, the FTC considered applying the rules to retailers that accept bank credit or debit cards and declined to do so. We believe that determination remains equally justified today.

Our Qualifications

Joel Winston served for 35 years in the FTC's Bureau of Consumer Protection. For nine years, he headed the FTC's offices responsible for consumer information privacy and security, serving as Associate Director for Financial Practices (2000-2005) and for Privacy and Identity Protection (2005-2009). His responsibilities included the development of the FTC Safeguards Rule in 2000-2001, and he directed the FTC's enforcement of that Rule and other consumer protection laws.

[2] Bank-issued payment cards include credit cards, debit cards and prepaid cards.

Anne Fortney has 39 years' experience in the consumer financial services field, including directing FTC enforcement and rulemaking under the federal consumer financial protection laws as the Associate Director for Credit Practices of the Bureau of Consumer Protection.

We both regularly counsel consumer financial services clients on their compliance obligations. We also assist clients in Consumer Financial Protection Bureau ("CFPB") examinations and in the defense of FTC and CFPB investigations and enforcement actions. In addition, we have each testified multiple times as invited witnesses before U.S. Congressional Committees and Subcommittees on various consumer financial protection laws. We each serve from time to time as subject matter experts in litigation in the federal courts involving consumer financial services.

Background

Federal Requirements for Safeguarding Customer Information

Section 501(b) of the Gramm-Leach Bliley Act ("GLBA" or the "Act")[3] required each of the federal bank regulatory agencies (the "Agencies")[4] and the FTC to establish standards for the financial institutions subject to their respective jurisdictions with respect to safeguarding consumers' nonpublic, personal financial information. The Act required that the safeguards ensure the security and confidentiality of customer records and information; protect against any anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer.[5]

Interagency Guidelines

Because they exercise supervisory responsibilities over banks through periodic examinations, the Agencies issued their GLBA customer information safeguard standards in the form of Guideline document ("Interagency Guidelines" or "Guidelines"). [6]

The Guidelines instruct banks on specific factors that serve as the basis for the Agencies' review during supervisory examinations. They are predicated on banks' direct control over the security of their customers' nonpublic personal financial information.

---

[3] Gramm-Leach-Bliley Financial Modernization Act, Pub. L. 106–102, § 501(b) (1999), codified at 15 U.S.C.A. § 6801(b).

[4] These were the Office of the Comptroller of the Currency ("OCC"), the Board of Governors of the Federal Reserve System ("FRB"), the Federal Deposit Insurance Corporation ("FDIC"), and the Office of Thrift Supervision ("OTS"). In October 2011, as a result of the Dodd-Frank Wall Street Reform and Consumer Protection Act, the OTS was terminated and its functions merged into the OCC, FRB, and FDIC.

[5] 15 U.S.C.A. § 6801(b).

[6] Interagency Guidelines Establishing Information Security Standards, 66 Fed. Reg. 8616-01 (Feb. 1, 2001) and 69 Fed. Reg. 77610-01 (Dec. 28, 2004) promulgating and amending 12 C.F.R. Part 30, app. B (OCC); 12 C.F.R. Part 208, app. D-2 and Part 225, app. F (FRB); 12 C.F.R. Part 364, app. B (FDIC); and 12 C.F.R. Part 570, app. B (OTS). The Agencies later issued an interpretive Interagency Guidelines on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 Fed. Reg. 15736-01 (Mar. 29, 2005). This paper includes this interpretive Interagency Guidelines in the summary of the Interagency Guidelines.

They instruct each bank to implement a comprehensive written information security program, appropriate to its size and complexity, that: (1) insures the security and confidentiality of consumer information; (2) protects against any anticipated threats or hazards to the security or integrity of such information; and (3) protects against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

The Guidelines provide specific instructions for banks in the development and implementation of an information security program. A bank must:

- Involve the Board of Directors, which must approve the information security program and oversee the development, implementation and maintenance of the program;
- Assess risk, including reasonably foreseeable internal and external threats, the likelihood and potential damage of these threats, and the sufficiency of the bank's policies and procedures in place to control risk;
- Design the program to control identified risks. Each bank must consider whether the following security measures are appropriate for the bank, and, if so, adopt the measures it concludes are appropriate:
    - Access controls on customer information systems;
    - Access restrictions at physical locations containing customer information;
    - Encryption of electronic customer information;
    - Procedures designed to ensure that customer information system modifications are consistent with the bank's information security program;
    - Dual control procedures,
    - Segregation of duties, and employee background checks for employees responsible for customer information;
    - Response programs that specify actions to be taken when the bank suspects or detects unauthorized access to customer information systems, including appropriate reports to regulatory and law enforcement agencies; and
    - Measures to protect against destruction, loss, or damage of customer information due to potential environmental hazards;
- Train staff to implement the information security program;
- Regularly test key controls, systems, and procedures of the information security program;
- Develop, implement, and maintain appropriate measures to properly dispose of customer information and consumer information;
- Adequately oversee service provider arrangements, including by contractually requiring service providers to implement appropriate procedures and monitoring service providers;
- Adjust the program in light of relevant changes in technology, sensitivity of consumer information, internal and external threats, the bank's own changing business arrangements, and changes to customer information systems;
- Report to the Board of Directors at least annually; and

- Provide for responses to data breaches involving sensitive customer information,[7] which should include –
    - Developing a response program as a key part of its information security program, which includes, at a minimum, procedures for assessing the nature and scope of an incident;
    - Notifying the bank's primary federal regulator as soon as the bank becomes aware of the breach;
    - Notifying appropriate law enforcement authorities;
    - Containing and controlling the incident to prevent further unauthorized access to or use of consumer information; and
    - Notifying consumers of a breach when the bank becomes aware of an incident of unauthorized access to sensitive customer information. The notice must include certain content and must be given in a clear and conspicuous manner and delivered in any manner designed to ensure the customer can reasonably be expected to receive it.

FTC Safeguards Rule[8]

The FTC protects consumers against "unfair and deceptive acts and practices in or affecting commerce."[9] Its jurisdiction includes "all persons, partnerships, or corporations," except banks, savings and loan institutions, federal credit unions and certain nonfinancial entities regulated by other federal agencies.[10] The FTC issues substantive rules, such as the Safeguards Rule, when required by Congress to do so,[11] but it is not authorized to conduct supervisory examinations of entities under its broad jurisdiction. Rather, the FTC is primarily a law enforcement agency.

Because the FTC lacks supervisory examination authority, it issued a Safeguards Rule, rather than Guidelines, to establish customer information safeguards for "financial institutions" under its jurisdiction. The GLBA's broad definition of "financial institution" includes a myriad of nonbank companies that operate in the consumer financial services industry.[12] The definition includes finance companies, auto dealers, debt collectors and consumer reporting agencies,

[7] Sensitive customer information includes: a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's account, and any combination of components of customer information that would allow someone to log onto or access the customer's account (i.e., user name and password, or password and account number). 12 C.F.R. Part 30, app. B, supp. A, § III.A.1; 12 C.F.R. Part 208, app. D-2, supp. A, § III.A.1, and Part 225, app. F, supp. A, § III.A.1; 12 C.F.R. Part 364, app. B, supp. A, § III.A.1; and 12 C.F.R. Part 570, app. B, supp. A, § III.A.1.

[8] FTC Safeguards Rule, 16 CFR Part 314. The FTC issued the final rule in 2001.

[9] 15 U.S.C.A. § 45(a)(1). The FTC Act also prohibits unfair methods of competition in or affecting commerce.

[10] 15 U.S.C.A. § 45(a)(2). For example, the FTC Act exempts not-for-profit entities and common carriers subject to the Communications Act of 1934.

[9] The FTC has more general rulemaking authority under Section 18 of the FTC Act, 15 U.S.C.A. § 57a, but has promulgated very few rules under that section in recent years.

[12] *See* 15 U.S.C.A. § 6809(3) (defining "financial institution" to include any institution engaging in "financial activities"); 12 U.S.C.A. § 1843(k) (defining "financial activities" broadly to include activities that are "financial in nature or incidental to such financial activity" or "complementary to a financial activity").

among many others. The FTC determined that the final Rule would not apply to retailers that merely accept payment cards, but rather, only to those that extend credit themselves, and only then to the extent of their credit granting activities.[13]

In recognition of the great variety of businesses covered by the Safeguards Rule, the FTC developed a rule that provided for flexible safeguard procedures that could be adapted to the myriad ways in which covered entities are structured and operate. The FTC Rule requires a financial institution to develop, implement, and maintain a comprehensive written information security program that contains safeguards that are appropriate to the entity's size and complexity, the nature and scope of its activities, the types of risks it faces, and the sensitivity of the customer information it collects and maintains. The information security program must: (1) ensure the security and confidentiality of consumer information; (2) protect against any anticipated threats or hazards to the security or integrity of such information; and (3) protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to any customer.

In its development, implementation, and maintenance of the information security program, the financial institution must:

- Designate an employee or employees to coordinate the program;
- Identify reasonably foreseeable internal and external risks to data security and assess the sufficiency of safeguards in place to control those risks in each relevant area of the financial institution's operations (i.e., employee training, information systems, prevention/response measures for attacks);
- For all relevant areas of the institution's operations, design and implement information safeguards to control the risks identified in the risk assessment, and regularly test and monitor the effectiveness of key controls, systems, and procedures;
- Oversee service providers, including by requiring service providers to implement and maintain safeguards for customer information; and
- Evaluate and adjust the program in light of material changes to the institution's business that may affect its safeguards.

[13] *See* 16 C.F.R. §§ 314.2(a) (adopting the Privacy Rule's definition of "financial institution"). That definition includes examples of "financial institutions," among them: retailers that extend credit by issuing their own credit cards directly to consumers; businesses that print and sell checks for consumers; businesses that regularly wire money to and from consumers; check cashing businesses; accountants; real estate settlement service providers; mortgage brokers; and investment advisors 16 C.F.R. § 313.3(k)(2). The FTC also opined that debt collectors are "financial institutions." 65 Fed Reg. 33646; 33655 (May 24, 2000). Further, the Privacy Rule also gives examples of entities that are ***not*** "financial institutions": retailers that only extend credit via occasional "lay away" and deferred payment plans or accept payment by means of credit cards issued by others; retailers that accept payment in the form of cash, checks, or credit cards that the retailer did not issue; merchants that allow customers to "run a tab"; and grocery stores that allow customers to cash a check or write a check for a higher amount than the grocery purchase and obtain cash in return. *Id*. at (k)(3).

When it promulgated this rule, the FTC considered requiring more specific and detailed data security requirements, but determined that doing so would have imposed significant regulatory burdens in light of the broad range of entities potentially subject to the Safeguards Rule.

Comparison of the Interagency Guidelines and the FTC Rule

Both the Interagency Guidelines and the FTC Rule apply only to "financial institutions" with respect to the "nonpublic personal" financial information they collect and maintain. Unlike the Guidelines, however, the FTC Rule applies to many types of entities whose principal business may not involve the provision of financial services to consumers.

While the Guidelines and the FTC Rule share some common elements, they differ in critical respects. In particular, the Interagency Guidelines, which are tailored to closely supervised and regulated banks, are much more detailed in their requirements. These requirements are designed to be the point of reference in an interactive process between the banks and their examiners. As their name implies, the Guidelines are intended to guide banks' compliance on a going forward basis.

In contrast, the FTC Rule is significantly less specific in its data security requirements than the Guidelines, because the Rule applies to a much broader and more diverse group of entities with wider variations in the data they collect and maintain, the risks they face, and the tools they have available to address those risks. The more general requirements of the FTC Rule also are designed to be adaptable to the near-constant changes in threats, security technologies, and other evolutionary developments in this extremely dynamic area. Whereas the Agencies can address new developments through the interactive examination process, the FTC only has the blunt instrument of law enforcement. And, whereas the Agencies actively supervise and monitor the activities of the entities they oversee, the FTC can only investigate and, if appropriate, take enforcement action against a fraction of the entities over which it has jurisdiction. The FTC's primary focus is on prosecuting past or existing deficiencies, and a company may receive no advance warning of a possible violation of the Safeguards Rule until it is confronted with an adversarial investigation. The Agencies' goal, on the other hand, is to prevent future deficiencies by working with the bank on an ongoing basis.

Effect of an FTC Standard That Would Apply Interagency Guidelines to Nonbanks That Do Not Extend Credit and Only Accept Credit Cards

For several reasons, safeguards requirements designed for closely supervised banks that issue credit and debit cards are a poor fit for the vast array of entities that accept credit cards and debit cards as payment for their goods and services. First, as explained above, the Guidelines are premised on an ongoing and interactive process between regulator and regulated entity, whereby examiners can instruct a bank on an apparent failure to meet a specific requirement. This process enables the institution to explain why a particular element of the Guidelines may be inapplicable or to correct any real deficiencies without legal sanctions.

No such process is possible for entities subject to FTC oversight. The FTC obtains compliance by initiating law enforcement investigations, using compulsory process, when it suspects a potential law violation based on facts that have come to its attention. This "after the fact" review focuses, through an adversarial process, on the legal requirements or prohibitions that may have been violated. If violations are found, the FTC seeks a formal order prohibiting the illegal conduct and, in appropriate cases, imposing fines or redress to injured consumers. The FTC lacks supervisory examination authority and lacks the resources to provide the specific guidance and ongoing oversight that would be necessary to effectuate Guidelines-type rules covering the huge diversity of nonbank entities. The result would be comparable to the widespread confusion and noncompliance that resulted from the FTC's attempt to so broadly define "creditors" subject to its Red Flags Rule[14] that the Rule would apply to types of businesses (such as plumbers, dry cleaners, hospitals, and restaurants) for which the Rule requirements made little sense. Congress had to correct that result with legislation that "reined in" the FTC by limiting the rule to the kinds of "creditors" that need written procedures to detect and prevent identity theft, rather than virtually every consumer-facing business.[15]

Second, many of the specific requirements of the Guidelines simply are not relevant to, or would impose unreasonable obligations on, nonbanks. For example, with respect to credit and debit cards, the Guidelines' obligations are premised on the specific circumstances and capabilities of card ***issuers***, which differ substantially from those of entities that accept cards as payment. It is the card issuers, and not the card-accepting merchants, be they hotels or veterinarians, that dictate the card processing capabilities of the equipment and procedures that merchants must use, as well as the security features inherent in the cards. Although chip and PIN technology could reduce card fraud, and many retailers have demonstrated a willingness to install terminals to accept cards with that technology, only card-issuing financial institutions can decide whether to issue fraud-resistant chip and PIN cards. Were the FTC required to enforce safeguard standards for credit and debit card data based on the Guidelines' model, it would be imposing obligations on the entities with the least ability to ensure that they were carried out.

Finally, it is important to note that nonbanks, although not covered by the Safeguards Rule, are subject to the FTC's general authority under Section 5 of the FTC Act to prohibit unfair or deceptive practices. The FTC has used this authority to prosecute dozens of nonbanks for engaging in the same practices proscribed by the Safeguards Rule, i.e., failing to take reasonable measures to protect consumers' personally identifiable information.[16] Thus, it is unclear what

[14] *See* 16 C.F.R. Parts 681.1(b)(4), (5) (2009) (effective until February 11, 2013) (referring to 15 U.S.C.A. § 1691a(r)(5) (the Equal Credit Opportunity Act), which defines "creditor" as, among other things, "any person who regularly extends, renews, or continues credit," and defines "credit" as "the right granted by a creditor to a debtor to… ***purchase property or services and defer payment therefor***") (emphasis added).
[15] Red Flag Program Clarification Act of 2010, Pub. L. 111-319, § 2 (2010).
[16] *See, e.g., FTC v. Wyndham Worldwide Corp., et al.*, No. CV 12-1365-PHXPGR, in the U.S. District Court for the District of Arizona (2012); *In the Matter of Fandango, LLC*, Matter Number 132 3089 (2014); ***In the Matter of Cbr Systems, Inc***., Matter Number: 112 3120 (2013); *In the Matter of Dave & Buster's, Inc.*, Matter Number 082 3153

additional benefit to the public would gain by subjecting nonbanks to specific requirements of the Guidelines.

As noted earlier, when issuing the GLBA rules, including the Safeguards Rule, the FTC specifically considered whether the rules should apply to retailers that accept bank-issued credit cards but do not extend credit themselves. The FTC correctly concluded that to do so would constitute a significant expansion of the FTC's authority to encompass the regulation of any transaction involving acceptance of a payment, whether cash, cards, checks or otherwise.

(2010); *In the Matter of CVS Caremark Corp.*, Matter Number: 072-3119 (2009); *In the Matter of Gencia Corp. and Compgeeks.com d/b/a computer Geeks Discount Outlet and Geeks.com*, Matter Number: 082 3113 (2009); *In the Matter of TJX Companies*, Matter Number: 072-3055 (2008); *In the Matter of Life is good, Inc. and Life is good Retail, Inc.*, Matter Number: 0723046 (2008); *U.S. v. ValueClick, Inc., et al.*, No. CV 08-01711, in the U.S. District Court for the Central District of California (2008); *In the Matter of Guidelines Software, Inc.*, Matter Number: 062 3057 (2007); *In the Matter of CardSystems Solutions, Inc.*, Matter Number: 052 3148 (2006); *In the Matter of DSW Inc.*, Matter Number: 052 3096 (2006); *In the Matter of BJ's Wholesale Club, Inc.*, Matter Number: 042 3160 (2005); *In the Matter of Petco Animal Supplies, Inc.*, Matter Number: 0323221 (2005); *In the Matter of Guess?, Inc. and Guess.com, Inc.*, Matter Number: 022 3260 (2003). These actions are in addition to those that the FTC has brought under the GLBA Safeguards Rule and/or the Consumer Information Disposal Rule. *See, e.g.*, *U.S. v. PLS Financial Services, Inc., et al.*, Case No. 1:12-cv-08334, in the U.S. District Court for the Northern District of Illinois, Eastern Division (2012); *In the Matter of James B. Nutter & Company*, Matter Number: 0723108 (2009); *In the Matter of Premier Capital Lending*, Matter Number: 072 3004 (2008); *U.S. v. American United Mortgage Co.*, Civil Action No. 07C 7064, in the U.S. District Court for the Northern District of Illinois, Eastern Division (2007); *In the Matter of Nations Title Agency, Inc., et al.*, Matter Number: 052 3117 (2006).