STATEMENT OF

DAVID FRENCH
SENIOR VICE PRESIDENT, GOVERNMENT RELATIONS
NATIONAL RETAIL FEDERATION

FOR THE

HOUSE COMMITTEE ON FINANCIAL SERVICES
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

HEARING ON

"LEGISLATIVE PROPOSALS TO REFORM THE CURRENT DATA SECURITY AND BREACH NOTIFICATION REGULATORY REGIME"

MARCH 7, 2018

National Retail Federation
1101 New York Ave., NW
Washington, DC 20005
(202) 783-7891
www.nrf.com

EXECUTIVE SUMMARY

Our full statement appears in the following pages, but the key elements of our statement may be summarized as follows:

1. **Breaches occur everywhere. All businesses should have breach disclosure requirements.**
   - Breaches occur most often where very sensitive data that is highly valuable to thieves can be acquired, such as from financial institutions and the government.
   - According to the *2017 Data Breach Investigations Report*, published by Verizon, the financial services sector suffers about one-quarter of all breaches annually. This study examines ***where*** breaches occur, not just which businesses ***report*** breaches – an important distinction considering that not all industries are required to report their breaches.
   - Any comprehensive federal legislation should therefore require all financial institutions and other businesses to disclose breaches of sensitive data when they occur.

2. **Under today's banking laws, financial institutions can keep their data breaches secret.**
   - The Gramm-Leach-Bliley Act of 1999 predates the first state breach notification law by three years and does not require financial institutions to provide notice of their breaches.
   - Regulatory guidance issued in 2005 to interpret the law also does not require financial institutions to make data breach disclosures, leaving disclosure to their discretion.
   - The proposed legislation deems financial institutions' ***discretionary*** guidance regime as meeting the bill's ***mandatory*** requirement for covered entities to disclose breaches.
   - The Committee should fix this "notice hole" in its breach legislation moving forward.

3. **Data security requirements should be reasonable and appropriate for each business.**
   - Mandatory requirements to protect sensitive information should take into account the nature of the business being regulated, the sensitivity of the data it handles, and the extent to which it processes, or engages in transactions with, the most sensitive information.
   - "One-size-fits-all" data security regulation, as proposed in legislation, is not appropriate for the vast array of American businesses to be covered. This bill would place mandatory security requirements on all businesses that were designed for financial institutions with $10 billion or more in assets and handling the most sensitive financial information.
   - Retailers support legislation embodying a risk-based approach recommended by security experts and already adopted by the Federal Trade Commission (FTC). The FTC has brought more than fifty actions against businesses that fail to protect data at the level reasonable and appropriate for that business and the sensitivity of the data they handle.

4. **Improving the security of payment cards themselves would help reduce card breaches.**
   - If banks issued Chip-and-PIN cards in the U.S. as they do globally, the incentive for hackers to steal card data and the number of breaches would be dramatically reduced.
   - New EMV chip-and-*signature* cards do not stop lost or stolen card numbers from being used online or in stores, so the incentive for criminals to steal card numbers remains.
   - If U.S. banks required PINs to approve transactions, as they do around the world, card numbers could be rendered useless to would-be thieves, reducing their incentive to steal.
   - Like ATM transactions, requiring PIN-level security for credit and debit card purchases should be part of any comprehensive solution addressing data breaches.

Chairman Luetkemeyer, Ranking Member Clay, and members of the Subcommittee on Financial Institutions and Consumer Credit, on behalf of the National Retail Federation (NRF), I want to thank you for the opportunity to respectfully submit this statement for the hearing record and provide you with our views on legislative proposals to reform the current data security and breach notification regulatory regime, including the discussion draft of the "Data Acquisition and Technology Accountability and Security Act" circulated for stakeholders' review in February ("Discussion Draft"). Cybersecurity threats face every sector of the U.S. economy, and NRF supports comprehensive and achievable legislative solutions that Congress and the White House may work toward to better protect Americans' sensitive financial and personal data.

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.

A. Introduction

We appreciate the Subcommittee calling this hearing at a time when many kinds of American businesses find themselves the targets in an evolving war on our digital economy – a war in which they are unwilling combatants who must defend vigorously against attacks by both criminals and nation states. Key aspects of the cyberattacks facing the breadth of American industry sectors are, typically, the criminal fraud motive and the foreign source of the attack. Virtually all the data breaches we have seen in the United States during the past few years – from attacks on the networked systems of technology, retail, and entertainment companies that have been prominent in the news, to a reported series of attacks on our largest banks – have typically been perpetrated by overseas criminals who are breaking U.S. laws. These breached companies are victims of these external actors' crimes, and we should keep this in mind as we explore the issues discussed at the hearing and in forthcoming public policy initiatives related to this issue.

Retailers collectively spend billions of dollars safeguarding sensitive customer information and fighting fraud that results when criminals succeed in breaching their protected information systems. Data security is at the top of retailers' business priorities, and securing data from increasingly sophisticated attacks is an effort that our member companies, as a retail community, strive to improve every day. Data security is also an issue on which the retailer and consumer interests are aligned in the effort to protect the most sensitive information most retailers hold – the customer's payment card number. If retailers are not good custodians of payment data related to customers, they will no longer continue to frequent our establishments and use their credit and debit cards in our stores. When we examine the cybersecurity threats to all businesses, we should understand the basic underlying reason that retailers are being attacked is for payment card numbers in order to perpetrate card fraud.

We urge members of the Subcommittee to review and support legislative efforts designed to help mitigate the threat of cyberattacks as well as inform consumers of breaches of sensitive information *whenever* and *wherever* they occur. These issues are ones that we recommend you examine in a holistic fashion: we need to help prevent cyberattacks, and when attacks result in data breaches, help reduce fraud or other economic harm that may result from those breaches.

We should not be satisfied with simply determining what to do after a data breach occurs – that is, who to notify and how to assign liability. Instead, it is important to look at why such breaches occur, and what the perpetrators get out of them, so that we can find ways to reduce and prevent not only the breaches themselves, but the follow-on harm that is often the criminal motive behind these attacks. If breaches become less profitable to criminals, then they will dedicate fewer resources to committing them, and our data security goals will become more achievable.

With these guiding observations in mind, our statement below provides some initial comments on the Discussion Draft and the framework of proposed data security and breach notification legislation before this Subcommittee. We believe members of Congress and other Washington policymakers can work together to promote comprehensive breach legislation, which can be further bolstered by efforts within the private sector to improve data security practices outside of the lawmaking process. Retailers continue to invest in and promote technological security advancements, such as encryption and tokenization, that improve the security of our networks. We also believe there are ways to achieve greater security for the payment card itself since usable stolen card data is what drives the attacks on the retail industry networks. In our comments on proposed data breach legislation, we support several key elements that we believe would provide the best opportunity for Congress to establish a uniform, nationwide regime, based on the strong consensus of state laws, that applies to all businesses handling sensitive financial or personal information of consumers.

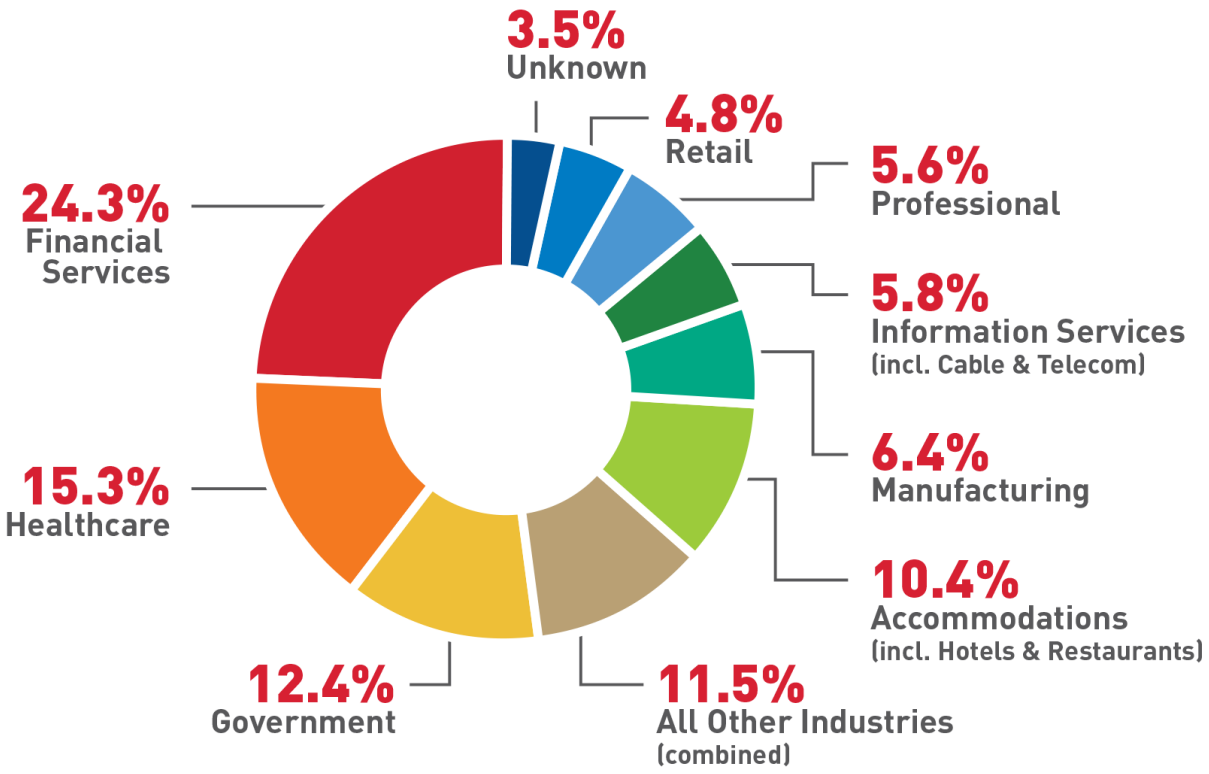
B. Where Breaches Happen Across Industry Sectors

Unfortunately, cyberattacks and 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 recently released *2017 Data Breach Investigations Report*,[1] Verizon examined 42,068 security incidents and 1,935 breaches, which it defines as security incidents resulting in "confirmed disclosure – not just potential exposure – of data to an authorized party."[2] It found that the financial services sector accounted for the most breaches of all industry sectors, with nearly a quarter (24.3%) of all breaches occurring in the sector in the past year. Specifically, the Verizon report examined 998 security incidents in the financial services sector, concluding that 471 of them constituted data breaches due to confirmed disclosure of data to an unauthorized party.

In its tenth year, Verizon calls its report "the most authoritative, data-driven cybersecurity report" because it "leverages the collective data from 65 organizations across the world." The Verizon breach report has been relied upon by investigators and analysts for a decade because it examines where breaches *occur* – including breaches undisclosed to the public – and does not just list which businesses publicly *report* having suffered a data breach. The report's coverage of undisclosed breaches as well as reported ones distinguishes it from other breach studies based on reported breaches – this distinction is important because some businesses, like retailers and restaurants, are *required* to report data breaches in 48 states and 4 federal jurisdictions, while others, like financial institutions, are not required by federal law or many state laws to do so.

[1] Verizon's *2017 Data Breach Investigations Report* is available at: http://www.verizonenterprise.com/verizon-insights-lab/dbir/
[2] Id., at p. ii.

The pie chart below illustrates where breaches occur, and it was created using the data in the Verizon report and, except for the "All Other Industries" category, uses the industry sector labels assigned by the report authors:



Source: Verizon 2017 Data Breach Investigations Report

The fact that more than half of all breaches occurred in just three sectors should not be a surprising revelation to Subcommittee members or staff when one considers that businesses in the financial services and healthcare sectors, along with U.S. government agencies, all handle American's most sensitive financial, health and identity information. The criminal hackers attacking the banks, healthcare providers and government agencies, as well as other types of businesses with similar sensitive information, know which data is most valuable to them and has the longest shelf life on the black market where the stolen data is sold to other criminals. Data thieves focus far more often on banks, which hold our most sensitive financial and personal 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.

As shown by the pie chart, businesses with less sensitive data generally account for fewer breaches because the data is less valuable to thieves. For instance, according to Verizon's report, the retail industry suffered just 4.8% of all breaches last year. Criminals are after the most valuable information they can find, and payment card numbers – which are immediately cancelled and replaced with new numbers when fraud is discovered – are not as valuable as bank account information that can lead to account takeovers and/or identity theft. It should also be noted that even these percentage figures above obscure the fact that there are far more merchants

that are potential targets of criminals in this area, as there are hundreds of times more merchants accepting card payments in the United States than there are financial institutions issuing cards and processing those payments.

Media reporting about data breaches is often disproportionate to the respective amount of security breaches in the banking and retail industry because, between them, only the retailers have strict, mandatory breach notification rules under all 48 state laws and 4 federal jurisdictions, including the District of Columbia, which require them to report data breaches whenever they occur. That is why consumers often hear far more about retail breaches in the news even though financial institutions have more than five times the number of breaches annually.

The latest breach report data from Verizon confirms the findings in many of its past reports, in that it reflects that significantly more data breaches occur at financial institutions than at retailers. What should be concerning to members of Congress and the public is that we rarely hear about any of the nearly five hundred security breaches in the financial services sector each year because banks, credit unions, and other financial institutions are not required to disclose them under federal banking law. The Equifax breach disclosure was the exception, not the rule.

Regardless of industry sector, there are far too many attacks that result in data breaches, and the breaches are often difficult to detect and are carried out in many cases by criminals with the latest technological methods at their disposal and significant resources behind them. We need to recognize that this is a continuous battle against determined fraudsters and be guided by that reality. It is also a key reason why our proposed solutions include a call to harden the payment card system and protections against card fraud. Without fraud-prone payment card information in a retailer's system, criminals would find the rest of the information retailers hold – benign data such as phone book information, shoe size, color preference, etc. – to be fairly uninteresting and, more importantly, relatively worthless on the black market.

C. Achievable Solutions to Improving Cybersecurity

As noted above, protecting their businesses and customers from cyberattacks is of paramount importance to retailers. In today's world of networked systems, the retail industry also recognizes that it is going to take the highest level of collaboration and coordination to make sure we do it right. That means government, industry and law enforcement alike must work together to address and defend against the attacks facing American businesses.

Retailers are committed to safeguarding consumer data and working with the federal agencies and Congress to achieve practical solutions to these serious problems. Over the past several years, we have outlined a specific set of achievable solutions that we – and every industry with a stake in the issue – must work toward to better protect American consumers, empower our businesses and effectively safeguard America's cyberspace against criminal hackers. Specifically, we have urged policymakers to work toward these solutions:

- Support the passage of FEDERAL FRAUD PROTECTION FOR DEBIT CARDS, similar to what consumers enjoy for credit cards. Americans should not have to pay more for fraud protection.

- Call on the payment card industry to stop relying on fraud-prone signatures and issue PIN AND CHIP CARDS for all Americans, among the least protected card-holders in the world.

- Encourage all entities in the payments system — not just retailers — to ADOPT END-TO-END ENCRYPTION to protect consumers' payment information throughout the entire payments chain.

- Endorse the development of OPEN, COMPETITIVE TOKENIZATION STANDARDS to replace consumers' sensitive personal data (including payment card data) with non-sensitive "tokens" so that stored information is useless to would-be hackers.

- Continue support for a SINGLE NATIONAL DATA BREACH NOTIFICATION LAW that would establish a clear disclosure standard for all businesses to inform consumers of breaches whenever and wherever they occur.

- Support the passage of federal law enforcement legislation that would AID IN THE INVESTIGATION AND PROSECURITON OF CRIMINIALS that breach our businesses' networks and harm our consumers.

In reviewing these proposals, we ask that you consider our views in each of these six areas of achievable solutions:

1. Federal Fraud Protection for Debit Cards

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

NRF supports legislation 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 concrete step Congress could take immediately to protect consumers that use debit cards for payment transactions.

2. Payment Card Security – "PIN and Chip" Cards

There are many technologies available that could reduce fraud resulting from payment card breaches, and an overhaul of the fraud-prone cards that are currently used in the U.S. market is long overdue. Simply using the best network security technology available does not guarantee that a business can avoid suffering a security breach which exposes sensitive data, such as payment card numbers. Therefore, raising security standards alone may not be the most efficient or effective means of preventing potential harm to consumers from card fraud. With respect to payment card numbers, for example, it is possible that no matter how much security is applied by

a business storing these numbers, the numbers may be stolen from a business's database in a highly sophisticated security breach that can evade even state-of-the-art system security measures. Because of these risks, it makes sense for industry to do more than just apply increased network or database security measures.

One method to help prevent downstream fraud from stolen card numbers is to require more data or additional numbers from a consumer (such as their entry of a 4-digit personal identification number, or "PIN") to complete a payment transaction rather than simply permit the transaction to be approved based on the numbers that appear on the face of a card. Requiring this type of out-of-wallet information to authorize and complete payment card transactions is time-tested by the banking industry, as they have required the use of PINs to access bank accounts through ATM machines for decades. Use of PINs has been a minor inconvenience that American consumers have borne for the trade-off in increased security when accessing cash. Around the globe, the most industrialized nations – the G-20 – have also adopted PIN-based solutions for card transactions to replace the antiquated signature authentication methods that derive from the mid-twentieth century.

NRF believes it is time to phase out signature-authentication for all U.S.-issued payment cards – today's magnetic stripe cards as well as tomorrow's chip-based cards – and adopt a more secure authentication method for credit and debit card transactions. PINs can provide an extra layer of security against downstream fraud even if the card numbers (which the card companies already emboss on the outside of a card) are stolen in a breach. In PIN-based transactions, for example, the stored 20-digits from the card would, alone, be insufficient to conduct a fraudulent transaction in a store without the 4-digit PIN known to the consumer and not present on the card itself. These business practice improvements are easier and quicker to implement than any new federal data security law, and they hold the promise of being more effective at preventing the kind of financial harm that could impact consumers as companies suffer data security breaches affecting payment cards in the future.

In support of these concepts, on October 17, 2014, President Obama signed an executive order initiating the BuySecure Initiative for government payment cards.[3] 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. Requiring PINs for all payment card transactions, as are required for some debit and ATM transactions (and some in-bank teller transactions as well) are common-sense actions that the banking industry should adopt immediately. Retail customers – American consumers – would be better protected by the replacement of a signature – a relic of the past – with the tried-and-true PIN that all other G-20 nations, including Canada, the U.K. and our European allies have adopted as part of their card payment system to protect their citizens.

As I noted, requiring the use of a PIN is one way to reduce fraud. Doing so takes a vulnerable piece of data (the card number) and makes it so that it cannot be used on its own. This approach to payment card security should be adopted not only in the brick-and-mortar

[3] 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

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, like methods being developed in Canada and Europe. Adopting PIN-like protections for online purchases may help directly with the high percentage of U.S. fraud which occurs online.

3. Network Security – "End-to-End Encryption"

Encryption of payment card transaction data is another technological solution retailers employ to help defend against cyberattacks and that could help deter and prevent data breaches and the resulting fraud that can occur. Merchants are already required by Payment Card Industry (PCI) data security standards to encrypt cardholder data while being stored but, as not everyone in the entire payments chain is able to accept data in encrypted form during payment authorization, sensitive data may be left exposed (after it leaves the retailer's system in encrypted form) at a critical time in the payment process. Payment security experts have therefore called for a change to require "end-to-end" (or "E2E") encryption, which is simply a way to describe requiring everyone in the payment-handling chain to accept, hold and transmit the payment card data in encrypted form. This would require, as the PCI standards currently require of merchants but not of others in the payment stream, that card-issuing banks, merchant banks, branded payment card networks and payment card processors all adopt the same technology to handle encrypted payment card data. In fact, knowing that card chip technology alone is not the panacea touted by branded payment card networks, many retailers are not waiting for an E2E standard, and are investing, at significant costs, in point-to-point (or "P2P") encryption.

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 in order to make use of it. We ask policymakers to urge our partners in the payments system, like we have, to adopt the most secure technologies to protect American consumers from card fraud. In the meantime, until all the stakeholders in the payments system adopt technology to enable "end-to-end" encryption, using PIN-authentication of payment cards now would offer some additional protection against fraud should the decrypted payment data today be intercepted by a criminal during its transmission "in the clear."

4. Open, Competitive Tokenization Standards

Another sensible and achievable proposal to deter and protect against the harm that may result from cyberattacks is to minimize the storage and use by businesses of the full set of unredacted and unencrypted payment card numbers necessary to complete a transaction – a data protection principle known as "data minimization." For example, a decade ago, the National Retail Federation asked the branded card networks and banks to lift the requirement that retailers store full payment card numbers for all transactions.

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 card data can be replaced, for example, 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.[4] Still, like the other proposed technological solutions above, tokenization is not a silver bullet solution, and it is important that whichever form of tokenization is adopted be one based on an open standard. This would help prevent a small number of networks from obtaining a competitive advantage, by design, over other payment platforms through the promotion of proprietary tokenization standards only.

In addition, in some configurations, mobile payments offer the promise of greater security as well. In the mobile setting, consumers would not need to have a physical payment card – and the mobile payments technology certainly would not need to replicate the security problem of physical cards that emboss account numbers on their face. It should also 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, and increasingly, biometric finger prints. Indeed, if we are looking to leapfrog the already aging and fraud-prone current technologies, mobile-driven payments may be the answer.

As much improved as they are, the EMV chips rolled out on U.S. payment cards are essentially dumb computers. Their dynamism makes them significantly more advanced than the magnetic stripes still present on most Americans' payment cards, but their sophistication pales in comparison with the sophistication of even the most common smartphone. Smartphones contain computing power that could easily enable state-of-the-art fraud protection technologies. Smart phones are nearly ubiquitous, and if their payment platforms are open and competitive, they will only get better.

5. National Data Breach Law

Each year the media is replete with news stories about data security breaches that raise concerns for all American consumers and for the businesses with which they frequently interact. Criminals focus on government agencies and U.S. businesses, including merchants, banks, telecom providers, cloud services providers, technology companies, and others. These criminals devoted substantial resources and expertise to breaching the most advanced data protection systems. Vigilance against these threats is necessary, but we need to focus on the underlying causes of breaches as much as we do on the effects of them.

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

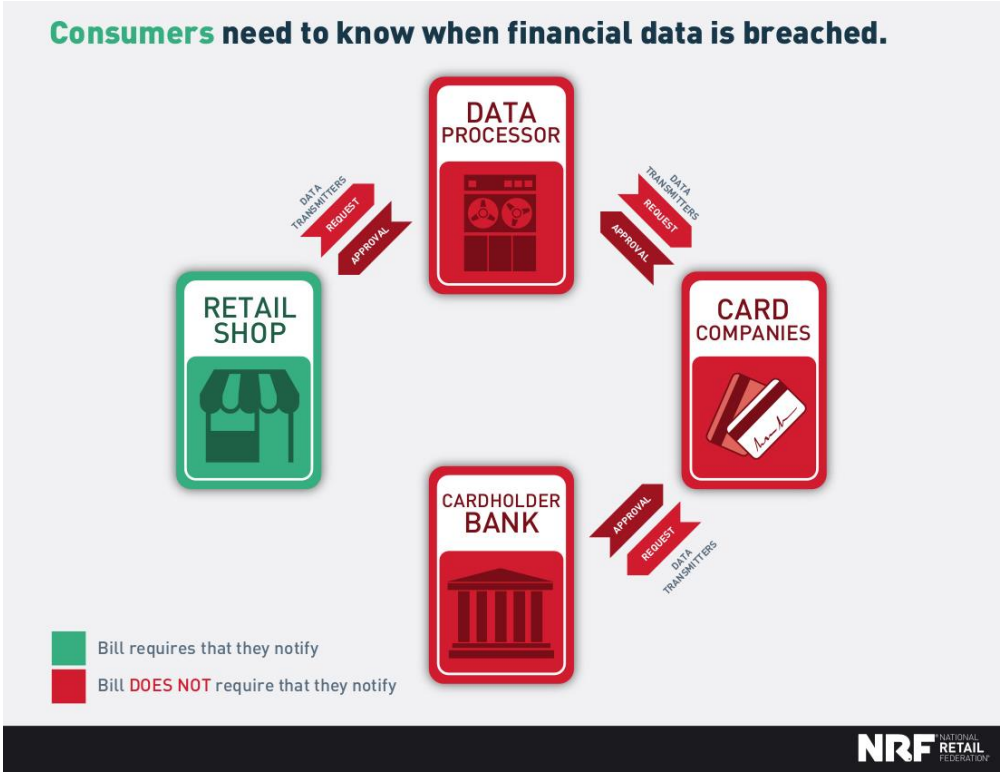
In fact, the safety of Americans' data is only as secure as the weakest link in the chain of entities that share that data for a multitude of purposes. For instance, when information moves

[4] 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.

across communications lines – for transmission or processing – or is stored in a "cloud," it would be senseless for legislation to exempt these service providers, if breached, from comparable data security and notification obligations that the law would place upon any other entity that suffers a breach. Likewise, data breach legislation should not subject businesses handling the same sensitive customer data to different sets of rules with different penalty regimes, as such a regulatory scheme could lead to inconsistent public notice and enforcement.

Given the breadth of these attacks, if Americans are to be adequately protected and informed, federal legislation must cover all 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. Indeed, Congress could establish the same data breach notice obligations for *all* entities handling sensitive data that suffer a breach of security. Congress should not permit "notice holes" – the situation where certain entities are exempt from reporting known breaches of their own systems. If we want meaningful incentives to increase security, everyone needs to have skin in the game.

The chart below, however, illustrates how some legislative proposals like the Discussion Draft would operate with respect to notice by financial institutions or a "third party" operating in the payment system. This graphic shows a typical payment card transaction in which a card is swiped at a card-accepting business, like a retail shop, the information is transmitted via communications carriers to a payment processor, which in turn processes and transmits the data to a branded card network, such as Visa or MasterCard, which in turn processes it and transmits it to the card-issuing bank. (Typically, there also is an acquirer bank adjacent to the processor in the system, which the chart omits to provide greater clarity of the general payment flows.)



As currently drafted, the Discussion Draft would only require the retail shop, in this example above, to provide consumer notice of a breach of security. The payment processor, transmitter of the payment data (e.g., telecommunications carrier), or card company suffering a breach would qualify as a third party under the bill 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. The card-issuing bank suffering a breach would be exempt from the notification obligations to consumers or the public under the Discussion Draft.

Compared to the figures in Verizon's 2017 Data Breach Investigations Report noted above, 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 payment system that suffers a breach, then 100% of the notices would come from the entities that suffer less than 5% of the breaches.

Breach Notification Exemptions for Financial Institutions

Many legislative proposals this Congress have "notice holes," where consumers would not receive disclosures of breaches by certain entities. Perhaps the notice hole that has been left unplugged in most proposals, including the Discussion Draft, is the exemption from notification standards for entities subject to the Gramm Leach Bliley Act (GLBA), which itself does not contain any statutory language that requires banks to provide notice of their security breaches to affected consumers or the public.

Interpretive information security guidelines issued by federal banking regulators in 2005 did not address this lack of a requirement when it set forth an essentially precatory standard for providing consumer notice in the event banks or credit unions were breached. Rather, the 2005 interagency guidelines state that banks and credit unions "should" conduct an investigation to determine whether consumers are at risk due to the breach and, if they determine there is such a risk, they "should" provide consumer notification of the breach.[5] These guidelines fall short of creating a notification *requirement* using mandatory language like "must" – an imperative command that could be used legislation to require breach notification for financial institutions. Instead, banks and credit unions are left to make their own determinations about when and whether to inform consumers of a data breach. **(In *Appendix A*, we have provided a two-page analysis of the use of "should" and other precatory language in the security guidelines that demonstrates there is no mandatory data breach notification requirement for financial institutions under GLBA or its interpretive guidance.)**

Several accounts 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 in 2014 that as many as one dozen financial institutions were targeted as part of the same cyberattack scheme.[6]

---

[5] 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

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

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 the affected institutions been made public. The lack of transparency and dearth of information regarding these incidents reflects the fact that banks are not subject to the same requirements to notify affected customers of their own breaches of security as other businesses are required now under 48 state laws. A few the more seasoned and robust state laws, such as California's breach notification law, have not exempted financial institutions from their state's breach notification law because they recognize that banks are not subject to any federal requirement that says requires them to notify customers in the event of a breach of security.

General Principle: The Breached Entity Should Have Notification Obligations

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

Some have called upon entities that are "closest to the consumer" to provide breach notice in all cases for any third party that handles data for that entity. As shown in the example above, however, we would suggest that the one-to-many relationships that exist in the payment card system and elsewhere will ultimately require potentially thousands of businesses to all notify about the same breach – another business's breach. This is not the type of transparent disclosure policy that Congress has typically sought.

An effort to promote relevant notices should not obscure transparency as to where a breakdown in the system has occurred. Indeed, a public notice obligation on all entities handling sensitive data would create significant incentives for every business that operates in our networked economy to invest in reasonable data security to protect the sensitive data in its custody. By contrast, a federal law that permits "notice holes" in a networked system of businesses handling the same sensitive personal information – requiring notice of some sectors, while leaving others largely exempt – will unfairly burden the former and unnecessarily betray the public's trust.

Data Security Standards

Data security standards vary depending on the nature of an entity's business and where it operates. Over the past half-century, the United States has essentially taken a sector-specific approach to data privacy requirements (including data security measures), and our current legal framework reflects this. For example, credit reporting agencies, financial institutions, and health care providers, just to name a few regulated sectors, have specific data security standards that flow from laws enacted by Congress, such as the Fair Credit Reporting Act (FCRA), the Gramm-Leach-Bliley Act (GLBA), and the Health Insurance Portability and Accountability Act (HIPAA), respectively.

The agencies that have implemented section 501(b) of GLBA—the Federal Financial Institutions Examination Council (FFIEC), the Office of the Comptroller of the Currency (OCC), the Federal Reserve Board (Fed Board), the Federal Deposit Insurance Corporation (FDIC), and the Office of Thrift Supervision (OTS)—have defined a process-based approach to security in the *Interagency Guidelines Establishing Information Security Standards* ("Security Guidelines")[7] Under the Security Guidelines, however, when designing security controls a financial institution is required to design an information security plan that "controls the identified risks, commensurate with the sensitivity of the information as well as the complexity and scope" of the entity's activities and, in so doing, must *consider* certain security measures and only if appropriate, adopt them.[8] Significantly, one of these security measures that a financial institution must consider, but is not required to adopt, is a "response program that specify actions to be taken when the institution suspects or detects that *unauthorized individuals have gained access to customer information systems*, including appropriate reports to regulatory and law enforcement agencies."[9] *(emphasis added)*

Those operating in other industry sectors that are subject to the jurisdiction of the Federal Trade Commission (FTC) must abide by the standards of care enforced by the FTC under Section 5 of the FTC Act, which give the Commission broad, discretionary authority to prosecute "unfair or deceptive acts or practices" (often referred to as their "UDAP" authority). On top of this federal statutory and regulatory framework, states have regulated businesses' data security practices across a variety of industry sectors and enforced consumer protection laws through their state consumer protection agencies and/or their attorneys general.

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

Effect of Imposing GLBA Guidelines for Financial Institutions as Mandatory Requirements on Commercial Businesses Subject to FTC Enforcement

NRF supports federal data security standards for all entities handling sensitive consumer information, but federal standards to be enforced by the FTC against the wide range of businesses under its jurisdiction would fall under the Commission's broad and discretionary authority to prohibit "unfair or deceptive acts or practices" and should be enforced consistent with the Commission's long-standing practices under Section 5 of the FTC Act.

---

[7] Interagency Guidelines Establishing Information Security Standards, 66 Fed. Reg. 8616 (Feb. 1, 2001) and 69 Fed. Reg. 77610 (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 (Board); 12 C.F.R. Part 364, app. B (FDIC); and 12 C.F.R. Part 570, app. B (OTS).
[8] *Id.* at ¶ III, C.1.
[9] *Id.* at ¶ III, C.1.g.

The FTC standard is consistent with the consumer protection standard that applies to financial institutions. Under Title X of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010, the Consumer Financial Protection Bureau (CFPB) was established and granted the authority to prohibit "unfair, deceptive or abusive acts or practices" for consumer financial products and services.[10] As the CFPB explains in the CFPB Supervision and Examination Manual, "Unfair, deceptive, or abusive acts and practices (UDAAPs) can cause significant financial injury to consumers, erode consumer confidence, and undermine the financial marketplace."[11] NRF is not aware of any financial institutions that have suggested that the CFPB standard is too weak.

Providing the FTC with different authority – to enforce process-based data security standards like those in the Security Guidelines implementing GLBA, as proposed in the Discussion Draft – would be an unprecedented and dramatic expansion of the FTC's authority that is unjustified in its application to the broad array of businesses subject to its jurisdiction. The Security Guidelines were designed for banking regulators that take an audit/examination approach to regulating companies and work with them through an iterative process to help the institution come into compliance where it may be lacking, without the threat of severe penalties. The FTC, by contrast, takes an enforcement approach, which under a GLBA-like guidelines standard, would require a post-hoc determination of a company's compliance with an amorphous standard in a world where the technological threat vectors are ever-changing.

In an adversarial investigatory process, like the kind the FTC employs in its enforcement of Section 5 of the FTC Act, entities are either guilty or not, and more likely to be guilty by the mere fact of a breach. Unlike financial institutions subject to the Security Guidelines, companies subject to FTC enforcement of its UDAP authority are not able to get several bites at the apple working with regulators until they know they are in compliance with the regulator's vision of data security. Rather, businesses facing FTC enforcement would have to guess at what will satisfy the agency and, if their security is breached, the strong enforcement presumption would be that the company failed to meet the subjective standard.

Because of this disparity in how security guidelines would be enforced, NRF sought an expert opinion on the effect of federal legislation that would impose banking industry-based data security standards on a vast array of commercial businesses, ranging from large nationwide companies to small, single-location businesses that are not "financial institutions." This would include every non-banking business in America that accepts virtually any form of tender other than cash (e.g., credit cards, debit cards, checks, etc.) in exchange for goods and services. **As part of your efforts to examine this issue, we strongly encourage you to review the white paper – attached as *Appendix B* to this testimony – that was prepared by two former associate directors responsible for financial and credit practices in the FTC's Bureau of Consumer Protection.** The authors' 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 business in the U.S. economy would be a

[10] The text of the Act is available at: http://www.gpo.gov/fdsys/pkg/PLAW-111publ203/pdf/PLAW-111publ203.pdf
[11] CFPB Supervision and Examination Manual, Version 2, October 2012, p. 174 (UDAAP 1), available at: http://www.consumerfinance.gov/f/201210_cfpb_supervision-and-examination-manual-v2.pdf

dramatic expansion of regulatory authority that is unprecedented in its scope and unjustified in its application.

Finally, the different enforcement regimes between financial institutions and entities subject to the FTC's jurisdiction is also evident in the manner and frequency with which fines are assessed and civil penalties imposed for non-compliance with a purported data security standard. Banks are rarely (if ever) fined by their regulators for data security weaknesses. But, as noted above, commercial companies have been fined repeatedly by the FTC. Providing an agency like the FTC, with an enforcement approach, a set of standards with significant room for interpretation is likely to lead to punitive actions that are different in kind and effect on entities within the FTC's jurisdiction than the way the standards would be utilized by banking regulators in an examination. A punitive approach to companies already victimized by a crime would not be appropriate nor constructive considering that the FTC itself has testified before Congress that no system – even the most protected one money can buy – is ever 100% secure.

Preemption – Establishing a Nationwide, Uniform Standard of Notification

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, 48 states and 4 other federal jurisdictions (including the District of Columbia and Puerto Rico) have enacted varying data breach notification laws. Many of the states have somewhat similar elements in their breach disclosure laws, including definitions of covered entities and covered data, notification triggers, timeliness of notification, 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 certain state officials be notified, and a few have time constraints (although the majority of state laws only require notice "without unreasonable delay" or a similar phrase.)

Over the past ten years, businesses such as retailers, to whom all the state and federal territory disclosure laws have applied, have met the burden of providing notice, even when they did not initially have sufficient information to notify affected individuals, through standardized substitute notification procedures in each state law. However, with an increasingly unwieldy and conflicting patchwork of disclosure laws covering more than 50 U.S. jurisdictions, it is time for Congress to acknowledge that the experimentation in legislation that 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 data moving 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.

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

In order to establish a uniform standard, preemptive federal legislation is necessary. But that does not mean (as some have contended) that the federal standard must or should be "weaker" than the state laws it would replace. On the contrary, in return for preemption, the federal law should reflect a strong consensus of the many state laws. Some have called for a more robust notification standard at the federal level than exists at the state level. Without adding unnecessary bells and whistles, NRF believes that Congress can create a stronger breach notification law by removing the exemptions and closing the types of "notice holes" that exist in several state laws, thereby establishing a breach notification standard that applies to all businesses. 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 Congress can work to enact a law with both robust protection and preemption.

We urge Congress, therefore, in pursuing enactment of federal breach notification legislation, to adopt a framework that applies to all entities handling sensitive personal information 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.

6. Greater Investigation and Prosecution of Cyber Criminals

In addition to the marketplace and technological solutions suggested above, NRF would also support a range of legislative solutions that we believe would help improve the security of our networked systems and ensure better law enforcement tools to address criminal intrusions.

Most important among these legislative solutions would be efforts to strengthen our extra-territorial law enforcement. As noted in our introduction above, industry sectors across the U.S. share the collective concern and face the same threat to their businesses' networks that appear to come predominantly from foreign actors. If the U.S. economy were threatened by foreign actors that had the most sophisticated technology to counterfeit our U.S. dollars, and were using it to perpetrate fraud in the United States and disrupt our economy, would Congress only be asking the victimized companies that unknowingly accepted counterfeit cash as payment why they did not better protect their customers from this fraud? We think that Congress, in this

hypothetical, would look first toward the criminal actors and enterprises that were perpetrating these crimes on our shores.

We therefore call upon Congress to develop legislation that would provide more tools to law enforcement to ensure that unauthorized network intrusions and other criminal data security breaches – particularly those with foreign attack signatures – 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.

C. Conclusion

Like financial institutions, American retailers are targets of cybercrime but suffer less than 5% of all security breaches. They do so predominantly because of the payment card data they accept and process. Criminals desire U.S.-based card numbers because they are unprotected and easily sold on the global black market to would-be fraudsters. The data thieves and their criminal customers – the purchasers of these stolen card numbers – realize the short lifespan of stolen card numbers once a breach is detected. That is why the criminals that hack American businesses typically go to extraordinary lengths to mask their incursions with methods that have not been seen before and that are not addressed by network security solutions. In short, if they can act undetected in this "cat-and-mouse" game, and place stolen card numbers on the black market before law enforcement and victimized businesses know the cards are there, they can drive up the market price for the stolen cards.

As stated earlier, retailers have invested billions in adopting data security technology. Efforts to promote payment card security, end-to-end encryption and tokenization are highlighted in the discussion above. The dominant card networks and card-issuing banks, however, have not made all the technological improvements suggested above that would make the payment 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. Our ability to improve payment card security and protect American consumers in the chain of the American payment ecosystem is, and will only be, as strong as its weakest link. Without the cooperation of our partners in the financial system, we cannot alone affect the changes necessary to better defend and protect against cyberattacks that lead to payment card fraud. Everyone already has skin in the game, and we need to work together to do what we can to improve an aging and outdated payment system that is the principal target of cyberattacks affecting U.S. retail businesses and their customers.

While everyone in the payments space has a responsibility to do what they can to protect against fraud and data theft that result from cyberattacks, there is much left for card-issuing banks and payment card networks to contribute, as retailers are doing, to better protect our payment system and the fraud-prone cards that are used in them. That is why we have proposed practical, commonsense and achievable solutions above that NRF believes are necessary to helping deter and defend against cyberattacks affecting the retail industry. We appreciate the opportunity to submit this statement to the Subcommittee today, and we look forward to working with the members of the Subcommittee and full Committee on Financial Services to bring greater attention to these issues and help push forward some or all of our proposed solutions to improve cybersecurity in across all industry sectors.

Appendix A:

Financial Institutions' Data Breach Notification Provisions under the Gramm-Leach-Bliley Act

Data Breach Notification Provisions and the Gramm-Leach-Bliley Act

Financial institutions are not required under federal law to notify customers of data breaches. While some have pointed to the Gramm-Leach-Bliley Act ("GLBA") as the source of such a requirement, the GLBA does not require notification of consumers of data breaches. The GLBA instructs the Office of the Comptroller of the Currency ("OCC"), the Federal Reserve Board ("Board"), the Federal Deposit Insurance Corporation ("FDIC"), and the Office of Thrift Supervision ("OTS") to establish "security and confidentiality" standards for financial institutions. Those agencies have developed guidelines, not regulations, to implement that part of GLBA.[1]

The bottom line is that there is no data breach notification provision or requirement under the Gramm-Leach-Bliley Act.[2] The guidelines established by the above agencies do not speak in mandatory terms. Instead they provide:

- When designing security controls, financial institutions need to "**consider**" a data breach response plan but are not required to develop a data breach response program or notify consumers after a breach.[3]

- According to the Incident Response Guide, financial institutions "**should**" have a data breach response program, but they are not required to have one.[4]

- "At a minimum, an institution's response program **should** contain procedures for…Notifying customers **when warranted**."[5] When notification is "warranted" is left to the discretion of the financial institution.

- "The proposed Guidance stated that an institution **should** notify affected customers whenever it becomes aware of unauthorized access to ''sensitive customer information'' unless the institution, after an appropriate investigation, reasonably concludes that misuse of the information is unlikely to occur . . ."[6]

- "The guidance is an **interpretation** of existing provisions in section 501(b) of the GLBA and Information Security Guidelines. Therefore, a delayed effective date is not required. Financial institutions **should** implement the interpretive guidance as soon as possible.

---

[1] *Interagency Guidelines Establishing Information Security Standards*, 66 Fed. Reg. 8616 (Feb. 1, 2001) and 69 Fed. Reg. 77610 (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 (Board); 12 C.F.R. Part 364, app. B (FDIC); and 12 C.F.R. Part 570, app. B (OTS) [hereinafter *Security Guidelines*]; *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) [hereinafter *Incident Response Guidance*].

[2] Gramm-Leach-Bliley Financial Services Modernization Act, Title V of the Financial Services Modernization Act of 1999, Pub. L. No. 106-102, 113 Stat. 1338 (Nov. 12, 1999) (*codified at* 15 U.S.C. §§ 6801, 6809, 6821, and 6827).

[3] *Security Guidelines*, *supra* note 3, at ¶ III, C.1.g.

[4] *Incident Response Guidance*, *supra* note 4, at ¶ II, A.

[5] *Incident Response Guidance*, 70 Fed. Reg. at 15740.

[6] *Incident Response Guidance*, 70 Fed. Reg. at 15743.

The agencies recognize that not every financial institution currently has a response program that is consistent with the interpretive guidance. The agencies will take into account the good faith efforts made by each institution to develop a response program that is consistent with the interpretive guidance, however; any financial institution experiencing a breach in security that includes unauthorized access to customer information is expected to respond promptly in a manner consistent with the guidance, and provide customer notice, **if warranted**."[7]

- "The final Guidance provides that when an institution becomes aware of an incident of unauthorized access to sensitive customer information, the institution **should** conduct a reasonable investigation to determine promptly the likelihood that the information has been or will be misused."[8]

- "If the institution determines that misuse of the information has occurred or is reasonably possible, it **should** notify affected customers as soon as possible."[9] So, even if a financial institution **knows** that stolen information has been misused, it is **still not required to notify** customers.

[7] Financial Institution Letter FIL-27-2005 (April 1, 2005) available at https://www.fdic.gov/news/news/financial/2005/fil2705.html.
[8] *Incident Response Guidance*, 70 Fed. Reg. at 15743.
[9] *Incident Response Guidance*, 70 Fed. Reg. at 15743.

Appendix B:

White Paper on Application of Safeguard Requirements for Banks to Nonfinancial Institutions

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).