Testimony

Submitted for the Record

from the

American Bankers Association

for the

Financial Institutions and Consumer Credit Subcommittee

of the

Committee on Financial Services

United States House of Representatives

Testimony

of the

American Bankers Association

for the

Financial Institutions and Consumer Credit Subcommittee

of the

Committee on Financial Services

United States House of Representative

March 7, 2018

Chairman Luetkemeyer, Ranking Member Clay, the American Bankers Association (ABA) is pleased to submit testimony on the importance of enacting a uniform federal data breach law to protect consumers across the nation. The ABA is the voice of the nation's $17 trillion banking industry, which is composed of small, mid-size, regional and large banks that together employ more than 2 million people, safeguard $13 trillion in deposits and extend more than $9.5 trillion in loans.

Protecting consumers in this increasingly sophisticated world of electronic commerce is a top priority of banks. It is clear that while our payments system remains strong, criminals continue to put consumers at risk by attempting to breach the security in almost every type of business and government agency. Banks and other financial institutions spend billions of dollars every year to protect consumers by investing in technology to detect and prevent fraud, reissuing cards and absorbing fraud costs. While the vast majority of payment card and other financial transactions are conducted safely, cyberattacks by criminals will continue against all businesses. If consumer financial information is stolen from retailers, businesses or banks, consumers have a right to swift, accurate, and effective notification of such breaches. They also should have confidence that, wherever they transact business electronically, the business is doing everything it can to prevent that breach from occurring in the first place.

Mr. Chairman, we strongly support your efforts to move forward on bipartisan data breach legislation. The ABA has consistently supported the following principles in legislation to provide stronger protection for consumer financial information:

1. Strong national data protection and consumer notification standards with effective enforcement provisions applicable to any party with access to important consumer financial information are critical. The costs of a data breach should ultimately be borne by the entity that incurs the breach.
2. Banks are already subject to robust data protection and notification requirements and that must be recognized.
3. In the event of a breach where consumers are at risk of harm, the public and other impacted parties should be informed as soon as reasonably possible.
4. State laws and regulations should be preempted in favor of strong Federal data protection and notification standards.

Banks are acknowledged leaders in defending against breaches. Therefore, from the financial services perspective, it is critical that data breach legislation takes a balanced approach that builds upon – ***but does not duplicate or undermine*** – what is already in place and highly effective in the financial sector.

The ABA is in the process of analyzing the Discussion Draft, and is likely to have further comments, but overall we are pleased that it addresses the critical goals that ABA members have advocated for many years and across several Congresses. ABA will continue to work with Congress to enact effective data security policies.

In this testimony we will focus on three main points:

- **The need for a national data breach standard.** Consumers' electronic payments are not confined by borders between states. As such, a national standard for data security and breach notification is of paramount importance.
- **The importance of recognizing existing Federal breach requirements.** Any Federal data protection and notification requirement must recognize existing national data protection and notification requirements.

- **The ABA's views on legislation.** Discussion Draft (the "Data Acquisition and Technology Accountability and Security Act") and the "PROTECT Act of 2017."

I. The Need for a National Data Breach Standard

Our existing national payments system serves hundreds of millions of consumers, retailers, businesses, banks, and the economy very well. Payments know no state border, nor does any cybercriminal. Therefore, a consistent national data breach policy is clearly necessary to effectively deal with the threats posed and protect customers.

Currently, 48 states, three U.S. territories, and the District of Columbia have enacted laws governing data security in some fashion, such as standards for data breach notification and for the safeguarding of consumer information. Although some of these laws are similar, many have inconsistent and conflicting standards, forcing businesses to comply with multiple regulations and leaving many consumers without protection and proper recourse. There is a better approach. Inconsistent state laws and regulations should be preempted in favor of strong Federal data protection and notification requirements. In the event of a breach, the public should be informed where it occurred as soon as reasonably possible to allow consumers to protect themselves from fraud.

Given the mobile nature of our nation's citizens, it is clear that the existing patchwork of state data breach laws are unduly complicated for consumers as well as businesses. For instance, consider a couple residing in a northern state who winter in a southern one and have their credit card data compromised at a merchant in a third state. In this instance, the couple wants to be alerted that their financial data has been compromised and that they are protected. Determining where the couple may or may not reside and which state laws may or may not apply unduly complicates the simple need to protect the couple from financial harm. It also diverts resources at the merchant and the bank toward determining how to comply with a myriad of laws as opposed to fixing the problem.

To limit the potential for data breaches in the first place, strong data protection requirements should be enacted that are applicable to any party with access to important consumer financial

information. Limiting the potential for such breaches through strong data protection is the first, essential, line of defense to maintain customer trust and confidence in the payments system.

Data security is also an ongoing process as opposed to the condition or state of controls at a point in time. Techniques of criminals change rapidly and prevention and mitigation efforts must as well. This is why ABA would oppose any mandated technology solution or specific security requirement which could soon become out of date and ineffective. A better approach, which is embodied in the Gramm-Leach-Bliley Act (GLBA) and the associated bank regulatory requirements, is to have a risk and governance-based approach rather than proscribing specific technological security requirements. Specifically, bank security programs are required to have "strong board and senior management level support, integration of security activities and controls throughout the organization's business processes, and clear accountability for carrying out security responsibilities."[1] Such an expectation is national in scope and should be treated that way.

II. The Importance of Recognizing Existing Federal Breach Requirements

Any legislation on data breach must also take into consideration the fact that some industries – ***including the financial industry*** – are already required by law to develop and maintain robust internal protections to combat and address criminal attacks, and are required to protect consumer financial information and notify consumers when a breach occurs within their systems that will put their customers at risk.

Title V of the GLBA requires banks to implement a "risk-based" response program to address instances of unauthorized access to customer information systems. At a minimum, a response program must:

1. Assess the nature and scope of any security incident and identify what customer information systems and customer information may have been accessed or misused;

[1] Federal Financial Institution Examination Council IT Handbook, available at http://ithandbook.ffiec.gov/it-booklets/information-security/introduction/overview.aspx

2. Notify the institution's primary federal regulator "as soon as possible" about any threats "to sensitive customer information."
3. Notify appropriate law enforcement authorities and file Suspicious Activity Reports in situations involving federal criminal violations requiring immediate attention;
4. Take appropriate steps to contain the incident to prevent further unauthorized access to or use of customer information, and
5. Notify customers "as soon as possible" if it is determined that misuse of customer information has occurred or is reasonably possible.

A critical component of the GLBA requirements is customer notification. When a covered financial institution becomes aware of a material breach of "sensitive customer information," it must conduct a reasonable investigation to determine whether the information has been or can be misused. If it determines that misuse of the information "has occurred or is reasonably possible," it must notify affected customers "as soon as possible."

Under GLBA, sensitive customer information includes the customer's name, address or telephone number in conjunction with the customer's Social Security number, driver's license number, credit card, debit card or other account number or personal identification number. Sensitive customer information also includes any combination of components of customer information that would allow someone to log onto or access the customer's account, such as user name and password.

A covered financial institution must also provide a clear and conspicuous notice. The notice must describe the incident in general terms and the type of customer information affected. It must also generally describe the institution's actions to protect the information from further unauthorized access and include a telephone number. The notice also must remind customers to remain vigilant over the next 12 to 24 months and to promptly report incidents of suspected identity theft to the institution.

Where appropriate, the notice also must include:

1. Recommendation to review account statements immediately and report suspicious activity;
2. Description of fraud alerts and how to place them;

3. Recommendation that the customer periodically obtain credit reports and have fraudulent information removed;
4. Explanation of how to receive a free credit report; and
5. Information about the FTC's identity theft guidance for consumers.

Banks that are engaged in the business of insurance marketing and sales face additional challenges with regard to data security because of the differences in the way banks and insurance companies are regulated. These differences can lead to duplicative and contradictory regulatory requirements for data security efforts.

Many financial institutions have affiliate agencies that can be housed in one of the three structures: in a bank itself, in a financial subsidiary of a bank, or in a nonbank subsidiary of a bank holding company (often a sister affiliate of the bank). Banks are heavily regulated with respect to the traditional products they offer – checking accounts, certificates of deposits, loans and lines of credit – so when it comes to data security, banks acting in their traditional roles must comply with a regulatory regime being established by banking regulators. Independent insurance agencies have their own set of rules they must follow, as established by state insurance regulators and that is the case for data security.

Consequently, when banks sell insurance – either directly or through an affiliated insurance agency – they face two different regulatory regimes: a regulatory regime that applies because they are banks, and a separate regulatory regime that applies because they are engaged in insurance. The current regulatory regime forces bank affiliated agencies to comply with contradictory regulatory requirements regarding data security. If an affiliate agency is operating in 48 states and a data breach takes place, the affiliate agency is forced to comply with 48 different data breach and notification standards as well as with federal regulatory requirements.

Within a bank holding company, cybersecurity is approached from the viewpoint of the entire holding company – not each affiliate individually. This is because the holding company may use a single information system for all of the affiliates within the holding company.

For these reasons, ABA recommends Congress pass legislation to allow data security and breach notification compliance by a bank holding company affiliate operating within the holding company's regulatory system (which satisfies all of the applicable bank regulatory requirements), to be deemed in compliance with federal law and to not be subject to duplicative regulation issued by state insurance authority pursuant to section 501(b) of the Gramm-Leach-Bliley Act.

These are strong standards that the financial services industry already must comply with.

As Congress contemplates data breach legislation, it is important that it build upon what is already in place and not duplicate or undermine what has already proven to be effective.

III. Discussion Draft, the "Data Acquisition and Technology Accountability and Security Act "

As mentioned at the outset, we strongly support Chairman Luetkemeyer and Representative Maloney's efforts to move forward on bipartisan data breach legislation. While we are still analyzing the full breadth of the Discussion Draft, we are pleased that it addresses the critical goals that ABA members have advocated for many years.

A. Data Protection

In particular, the data protection requirements in section 3 would put in place an effective data protection process for those that keep and use sensitive consumer information. Like the GLBA requirements that apply to financial institutions, every business must develop, implement and maintain reasonable administrative, technical and physical safeguards to protect sensitive personal information from unauthorized access and acquisition that is reasonably likely to result in identity theft, fraud or economic loss.

Also like GLBA, these safeguards must be appropriate to the size and complexity of the entity, the nature and scope of its activities, the cost of available tools to improve security and reduce vulnerabilities and very importantly, the sensitivity of the personal information it maintains. This makes implementing the safeguards a scalable and tailored process rather than a draconian, one-size fits all approach (which tends to hurt smaller businesses with fewer resources to draw upon).

The Draft provides guidance on what constitutes reasonable safeguards. For example, every company should delegate someone, either an owner, officer or employee, to oversee the safeguards that are put in place. The safeguards themselves are practical and basically what companies that are serious about data protection should be doing already. First, identify the internal and external security risks they face, and then implement safeguards designed to control those risks; ensure that any third parties they work with also protect the information; and evaluate and update everything as necessary for changes in technology and the threats to data security.

Any entity that obtains and uses a consumer's personal information should be required to protect it, no matter its size. However, there is no doubt that the approach taken in the Draft is

flexible and depends on what information is obtained and how it is used. Despite arguments to the contrary, there is clearly no intent to apply rigid standards to businesses that do not keep and use significant amounts of sensitive personal information.

B. Breach Notification

ABA has consistently supported strong data protection in order to prevent breaches as the first, and best, line of defense. However, if a breach does occur, consumers should be informed of the nature and extent of any fraud, identity theft or other risks they may face, as well as guidance on what they can do to protect themselves. GLBA has put that standard in place for banks and for years our members have taken the brunt of dealing with the costs and other aspects of breaches at retailers and other companies when they involve payment card and other information.

In fact, most of the time the press releases and other public notices sent out by breached companies tell consumers to contact their bank or credit union to find out what they can do to protect themselves. Often, the first time customers learn of a problem is when a bank has to reissue his or her credit or debit card. Many customers get confused and believe that the card was reissued because of something the bank has done wrong rather than the retailer or business where the breach actually occurred. Banks try to explain what happened and most often without much information about the actual breach. And banks end up footing the bill for the cost of the card and other anti-fraud efforts.

That is why we strongly support the provisions in section 4 of the Draft that in most instances make the breached company responsible for notifying consumers about the breach as soon as possible after it determines the scope and extent of the breach. There still appear to be some grey areas that need to be worked out and we would be concerned if changes are made that could allow those that have the ability to contact and inform consumers about a breach to avoid that obligation.

There is one other major aspect of the notice requirements that we would addressed. The timing of the notice has, and continues to be, the subject of debate. Clearly, looking at it from the consumer side of the equation, and from the perspective of banks and others that might be impacted by a breach, notice should be provided as quickly as possible. However, it is also

important to realize that every breach is different and that the exact scope of the breach, and exactly what personal information might have been put at risk, is generally not clear when a company first becomes aware that it has a problem. A certain amount of time and investigation is required to find out what happened and who should be notified.

In our view, it would be a mistake to put in place a time-certain for notification such as a certain number of hours or days. The standard set in the GLBA's requirements is "as soon as possible." While some states have specific maximum timelines, most are modeled on the GLBA standard although the exact language can differ. The reason for this is that consumers should be notified as soon as possible, but it is even more important that they are notified in a way that provides them with enough information to take effective action to protect themselves.

We think that the Draft attempts to balance this by providing that once the breached entity believes a breach of personal information may have occurred, it must conduct an immediate investigation to assess the nature and scope of the breach and take reasonable measures to restore security. After that, if there is a reasonable risk that the breach has, or could result in harm to the consumer the breached entity must notify law enforcement, appropriate regulators, consumers and other impacted entities "immediately and without unreasonable delay."

In addition, several safeguards are put in place such as a delay requested by law enforcement so that premature notification does not undermine the criminal investigation. There are also relatively low thresholds (5,000 or more consumers) for triggering notification to law enforcement, oversight agencies and the consumer credit reporting bureaus. In addition, there is guidance provided on the form of the notice and for how long the content must be kept available to consumers.

This timing language may require further discussion, but we would be very concerned if unrealistic timelines were to be added to the bill impacting financial institutions.

C. Oversight and Enforcement

One of the fundamental points ABA has strongly and consistently made is that banks are subject to oversight and examination for compliance with the GLBA data protection and notice requirements by several regulatory agencies. Depending on the bank's charter, the examinations are conducted by the Federal Reserve, the Office of the Comptroller of the Currency, the Federal

Deposit Insurance Corporation, or a combination of some or all of these agencies. It is more complicated than that, but what is clear is that every other bank in the country, has to prove it is in compliance with GLBA security and notice requirements and protecting our customers' data on a regular basis. There is no reason to duplicate that in another Federal law, and we are pleased that the Draft maintains that approach and leaves oversight and enforcement up to our prudential regulators.

With respect to non-banks, and certain financial institutions, the Federal Trade Commission (FTC) has historically had that oversight responsibility. The oversight of those companies is somewhat different than what we experience in that the FTC does ***not*** have examination authority. Instead, it relies on enforcing data protection requirements through consent orders after a breach has taken place. Section 5 of the Draft keeps that basic structure in place, but would also allow for the enforcement of the Federal data breach law by State Attorneys General.

D. Relation to State Law

As was mentioned earlier in this testimony, virtually every state has some sort of breach notification law in place, but only a small minority of states have enacted data protection laws. In our view, there needs to be a uniform standard for all states to better protect consumers and businesses across the nation. Our economy is nationwide, and in many cases global. It does not make sense to continue to address this issue through differing and often inconsistent state laws. It really should not matter where a consumer is located if their financial information has been compromised. A person living in one state should expect all businesses to respect and protect their financial information and to notify them when breaches have occurred—protection that should be consistent regardless of what state in which someone resides.

The Draft addresses this problem by both putting in place a strong federal data protection requirement that applies nationwide, and preempting "any state law, rule, regulation, requirement, standard or other provision, with respect to securing information from unauthorized access or acquisition." This makes sense from the perspective of the ABA and we would be concerned if this was not included in final legislation as it would amount to just another breach law on top of all the others already in place rather than real reform.

The legal, regulatory, examination and enforcement regime that is in place for banks ensures that banks robustly protect American's personal financial information. We believe that the

Discussion Draft provides an appropriate, scalable model for other businesses entrusted with sensitive customer financial and other information, and we strongly support your efforts to move forward on this important legislation.

Banks with affiliate agencies are often subject to oversight by the Office of the Comptroller of the Currency, the Federal Reserve, the FDIC, state banking regulators and state insurance regulators. The different regulatory regimes cause banks with affiliate agencies to be faced with contradictory regulatory requirements regarding data security and breach notification. ABA strongly supports a bank holding company affiliate operating within the holding company's regulatory system (which satisfies all of the applicable bank regulatory requirements), to be deemed in compliance with federal law and to not be subject to duplicative enforcement by state regulators.

IV. The PROTECT Act of 2017 (H.R. 4028)

Our understanding is that this bill has three basic parts and we have a few brief comments on each. Title I provides for the supervision and examination of large consumer reporting agencies by at least one of the Federal banking agencies. Although the data security standards of the GLBA apply to the credit bureaus, and they are subject to the FTC's oversight, they do not undergo rigorous bank-like examinations. Given the size of these organizations and the sensitivity of the information they keep, it would make sense for the Committee to consider this to better protect sensitive consumer information. ABA members would be concerned if this were to create additional compliance burdens on banks, but as far as we can tell this does not seem to be the case with respect to the provisions currently in the bill.

Title II would put in place various requirements that allow consumers to freeze, unfreeze and temporarily lift a credit freeze on their credit. Consumers are given a great deal of flexibility in how they make these requests and the credit bureaus have to meet certain time limits in implementing them. In the case of identity theft victims, active duty military, minors and senior citizens, they are free of charge. For others, a low fee can be charged. Overall, we do not see major problems if this were to be put in place. However, in experiences shared with us by bankers it could have an impact on the availability of credit for consumers that do not actively manage their frozen accounts.

Title III would prohibit the national credit bureaus from using social security numbers (SSNs) after January 1, 2020 in consumer reports, as a method for identifying a consumer and "for any other purpose." While we recognize that there is great concern about the use of stolen SSNs in general, and in particular with respect to the creation of synthetic "IDs," it is just not feasible to do this at this time for a number of reasons. The government and private sector use SSNs extensively, and an equivalent personal identifier does not exist. Thus, prohibiting the use of SSNs would (1) increase the potential for identify theft, (2) increase the cost not only of credit but other banking products, and (3) reduce the availability of credit and other banking services, all to the detriment of consumers. Creating a new, universal personal identifier and replacing the SSN cannot be achieved in the short time the bill demands. Moreover, whatever replaces the SSN simply becomes the new target with the same problems.

Our suggestions are to conduct a study of how and why SSNs are currently used by both the private sector and government and to identify ways to reduce their misuse and other options for verifying people's identity.

Conclusion

We appreciate the opportunity to present this testimony and to share our views on both the Discussion Draft and the PROTECT Act, and we look forward to working with you and the Members of the Committee on this important legislation.