March 7, 2018

Testimony of
Jason Kratovil

On behalf of

The Financial Services Roundtable

Before the

United States House of Representatives
Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit

Hearing entitled

"Legislative Proposals to Reform the Current Data Security and Breach Notification Regulatory Regime"

Chairman Luetkemeyer, Ranking Member Clay and Members of the Subcommittee, thank you for having me here today. On behalf of the leading banking and payments members of the Financial Services Roundtable, I appreciate the opportunity to discuss two very timely and important legislative proposals: A discussion draft of data security and consumer breach notification legislation titled the Data Acquisition and Technology Accountability and Security Act offered by the Chairman and Congresswoman Carolyn Maloney; and H.R. 4028, the Promoting Responsible Oversight of Transactions and Examinations of Credit Technology Act of 2017, or the PROTECT Act, offered by Congressman Patrick McHenry.

Data is increasingly the engine of modern commerce. For the financial services industry, the proliferation of data has been a catalyst to tremendous innovation. New technologies and analytical tools allow financial institutions of all sizes to assist their customers with financial management and retirement savings, for example, in more sophisticated and more secure ways than ever before.

For other sectors, economies of scale present far less of a barrier to entry today than they did even a decade ago, enabling the smallest firms to purchase the hardware and software – and engage the services of leading global technology and payments firms – to help them process and analyze data, provide better customer service and enhance business efficiencies.

Data held by private companies – and what can be extrapolated from that data – presents tremendous opportunity for consumers across the economy, but also raises new ethical, privacy and security questions as well.

The two proposals up for discussion today touch on the core of many of these questions: What companies have my data? How are those companies protecting it? If they lose my data will I find out, and when? What is the federal government's role in keeping my data secure?

<u>H.R. 4028, the PROTECT Act</u>

This legislation seeks to accomplish three goals: First, require supervision and examination of the cybersecurity practices of the nationwide credit reporting agencies (CRAs); second, create a nationwide standard for consumer security freezes on their credit reports; and third, prohibit the use of consumer Social Security numbers (SSNs) in a credit report or as a means to identify an individual consumer by CRAs effective January 1, 2020.

The nationwide CRAs play a vital role in the provisioning of credit to many American consumers. Their core product -- consumer credit reports – are multi-year retrospectives on how an individual managed their finances and how much credit he or she has been extended. It provides important insights for any financial institution seeking to evaluate the potential risk presented by an applicant for a variety of financial products, such as credit cards, mortgages, or personal loans. When a consumer wants to access a credit report, CRAs must attempt to *identify* (i.e. "Which 'John Smith' is requesting the file?") and *authenticate* ("Is this 'John Smith' actually who he says he is?") that individual to keep their file separate and distinct from every other individual on which they maintain a file. This requires a sophisticated identity proofing process based on a large body of knowledge specific to each individual consumer.

In other words, CRAs – understandably – hold a tremendous amount of information about every credit-active American consumer.

Consumer Reporting Agency Cybersecurity

CRAs are subject to the Federal Trade Commission's (FTC) authority under the Gramm-Leach-Bliley Act (GLBA) with respect to information security. Under the FTC's "Safeguards Rule," CRAs are required to have standards in place to safeguard customer information.[1] Title I of the PROTECT Act makes clear, however, that CRAs currently do not have proactive, ongoing oversight of their data security practices. Two observations:

- Banks, including their significant service providers, are subject to rigorous ongoing oversight and examination of their cybersecurity practices – in some cases by multiple regulatory bodies – and hold much of the same data on consumers as the CRAs. Thus:
- Mr. McHenry's proposal accurately identifies a gap – supervision and examination – that cannot be filled by the FTC in its capacity as an enforcement-only agency.

National Security Freeze

Every state and the District of Columbia have enacted legislation allowing consumers to place a freeze on their credit file.[2] In that respect, a national standard such as the one proposed in the PROTECT Act would smooth out the inconsistencies that currently exist

[1] See 16 CFR Part 314, accessed at: https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule

[2] http://www.ncsl.org/research/financial-services-and-commerce/consumer-report-security-freeze-state-statutes.aspx

across state laws. For consumers, it is reasonably certain that with a freeze in place a fraudster could not access a consumer's credit to commit identity theft.

However, there are also potential consumer disadvantages from having a credit freeze in place. For instance, it is also reasonably certain that with a freeze in place, it is not possible for the consumer to obtain credit at all. This can be very disruptive. For example, consumers very often encounter pressing needs or emergencies that may necessitate quick access to a new line of credit, which could be blocked if a consumer has not taken the appropriate steps or allowed sufficient time for the freeze to be lifted. Emergencies – car repairs or a broken water heater – or even routine transactions – buying a new mobile phone, financing the new bedroom set that finally went on sale – become impossible if the consumer forgot to "unfreeze" their file beforehand. Other tools exist – such as fraud alerts, credit monitoring, and the federally mandated availability of a free annual credit report – that may be more appropriate for many consumers.

Credit Rating Agency Use of Social Security Numbers

There is broad consensus among FSR members and beyond that the reliance on SSNs throughout the economy represents a broken system in need of reform. Fundamentally, SSNs were devised as a way to assist the federal government in dispensing benefits to the correct person. That they are now relied upon to both identify and, in many instances, authenticate a person (ostensibly because they are still a "secret") is a serious problem and increases their value to identity thieves. From a practical perspective, data breaches have exposed the SSNs of so many consumers that the case can be credibly made that everyone should stop pretending SSNs are any more confidential than information readily accessed in a phone book or five-second Internet search. [3] Recognizing this reality would make the continued use of SSNs *as identifiers* by CRAs and others far less problematic: The key is finding alternatives to the use of SSNs as *authenticators* of an individual, which requires much more effort.

To that end, the proposal to prohibit the use by CRAs of SSNs is certainly positive in driving a conversation on the future of digital identities. In fact, FSR members are actively engaged in charting a path toward a future built around trusted frameworks and standards for proving the identity of a person without a reliance on SSNs or passwords. Technological improvements will make this easier and firms are increasingly

[3] For more, see testimony of Jeremy Grant, Managing Director, Technology Business Strategy, Venable LLP before the U.S. House Committee on Energy & Commerce Subcommittee on Oversight and Investigations, hearing titled "Identity Verification in a Post-Breach World," 11/30/2017. Accessed at: http://docs.house.gov/meetings/IF/IF02/20171130/106662/HHRG-115-IF02-Wstate-GrantJ-20171130.pdf

experimenting with new methods that leverage behavioral data, biometrics, tokenization, geolocation and telematics, but this will take time to mature across the ecosystem.

Given the current state, I would make the following points to support our belief that the outright prohibition on SSN use as contemplated in the PROTECT Act is not advisable as a matter of legislative policy:

- First, viable alternative systems to replace SSNs are many years from becoming reality and will require not only significant work on the part of the private sector, but also the support and engagement of federal and state governments. Eventually, industry and government will develop new trusted methods to authenticate an individual that don't require SSNs, making their continued use as an identifier fairly harmless. Resources should be focused into these efforts, not into the scramble to find a new method of identifying a consumer that would inevitably be triggered were this measure to become law.
- Second, in many instances, the use of SSNs by financial institutions is required by federal rules and regulations. Unravelling SSNs from the fabric of financial services, as this measure would potentially require, will necessitate significant revisions to many federal rules and regulations that today obligate financial institutions to utilize SSNs to meet a variety of regulatory requirements.[4] That process will take time.
- Third, banning the use of SSNs as identifiers by the CRAs would make it very difficult for financial institutions to detect and stop instances of synthetic identity fraud.[5] This type of identity theft, which disproportionately affects the SSNs of children and is estimated to cost financial institutions $6 billion in losses each year,[6] can be dramatically reduced when institutions are able to verify whether or not a given name, date-of-birth and SSN correspond to what the SSA has on file. In fact, discussions are underway with Members of this Committee, your colleagues

[4] See Appendix A.

[5] Synthetic identity fraud involves the creation of a fake identity and credit file, often by using a combination of real data (most often SSNs of children) from multiple individuals and fabricated information. To carry out financial fraud, the fictitious identity and associated credit file is leveraged over time to build a positive history that allows the fraudster to ultimately apply for and obtain new credit. This new credit is quickly maxed out and, of course, never repaid. This immediate loss is absorbed by the financial institution. However, the child whose SSN was compromised may have no awareness that their information was used to commit synthetic identity theft until the first time he or she applies for credit, a student loan, etc., many years after the fraud has been committed. For more, please see: *"Why Children are now Prime Targets for Identity Theft,"* accessed at: http://thehill.com/opinion/cybersecurity/373692-why-children-are-now-prime-targets-for-identity-theft.

[6] "Synthetic Identity Fraud Cost Banks $6 Billion in 2016: Auriemma Consulting Group," *Markets Insider*, August 1, 2017. Accessed at: http://markets.businessinsider.com/news/stocks/synthetic-identity-fraud-cost-banks-6-billion-in-2016-auriemma-consulting-group-1002222563

on the Ways & Means Committee and in the Senate to modernize and enhance the ability of SSA to assist in fighting synthetic identity fraud. Senators Tim Scott (R-SC), Claire McCaskill (D-MO), Bill Cassidy (R-LA) and Gary Peters (D-MI) recently introduced the Protecting Children From Identity Theft Act, S. 2498, legislation that would help prevent synthetic identity fraud by improving the ability of financial institutions and CRAs to validate SSNs as consumer identifiers to flag and stop their misuse.

- Finally, CRAs are merely one segment of one sector of the economy. I would encourage policymakers to address this issue from a more holistic perspective: The overuse and over-reliance of SSNs is not limited to the CRAs, and prohibiting their use by this single slice of the economy is far from a cure to the overall problem. As mentioned, Congress has an essential role to play in facilitating public-private collaboration toward a set of solutions that works for every consumer and business in the United States that has a need to accurately verify their own identity, or the identity of a prospective customer. A piece-by-piece approach is likely to create more confusion and problems than it is likely to solve.

Discussion Draft: The Data Acquisition and Technology Accountability and Security Act

I have been engaged in this Committee's efforts on data security and consumer breach notification legislation in various capacities since the introduction of H.R. 3997, the Financial Data Protection Act of 2005, by my then-employer the late Rep. Steven C. LaTourette (R-OH), along with Reps. Darlene Hooley (D-OR), Mike Castle (R-DE), Deborah Pryce (R-OH) and Dennis Moore (D-KS). This first comprehensive, bipartisan bill passed this Committee but then, as has been the fate of every subsequent piece of data security legislation, could not be reconciled with competing legislation from the Energy & Commerce Committee and thus never reached the House floor.

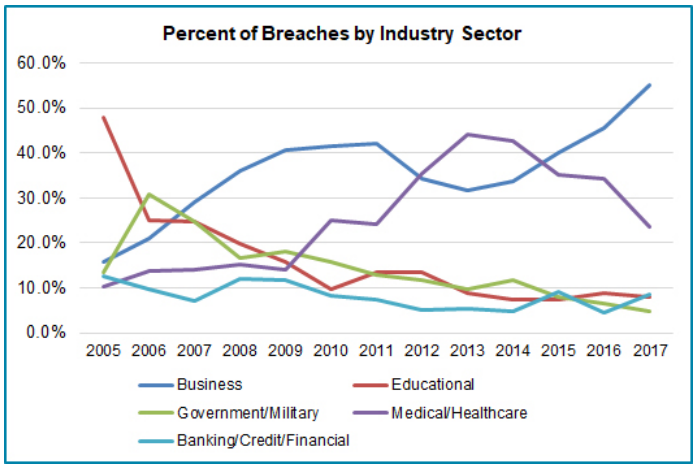
For 13 years, I and many others who have worked to advance federal data security legislation have watched as countless high-profile breaches came and went, each presenting an opportunity for Congress to respond, only to see bills fail to get beyond a single committee's process. Even in the last Congress, when legislation sponsored by Reps. Randy Neugebauer (R-TX) and John Carney (D-DE)[7] passed this Committee by an overwhelming vote of 46-9, that was not enough momentum to advance to the House floor.

[7] H.R. 2205, the Data Security Act of 2015.

Which begs the question, what will it take? To be sure, the devil most definitely is in the details when crafting strong federal legislation that strikes the right balance between protecting consumers with strong data protection requirements while providing timely, risk-based notification of a breach. Historically, this has led to divisions between industries that, unsurprisingly, followed jurisdictional lines between the relevant committees. While some of those divisions still remain, there is increasingly a desire among many industries to work together to support Congressional efforts to get a bill done. This was highlighted recently when 23 trade groups – representing financial services, technology, telecommunications and retail – signed a letter[8] to your colleagues on the House Energy & Commerce Committee outlining shared policy priorities. This was actually the first time such a broad group of industries has come together in any capacity on this issue. It is FSR's hope that finding consensus among these diverse stakeholders will help advance the efforts of this Committee and other committees of jurisdiction to advance legislation through the full House.

Overview

The entire financial services industry – from the leading members of FSR to the thousands of community banks and credit unions in this country – are united in our goal to protect consumers and prevent data breaches. Trust and confidence are hallmarks of our industry: Consumers have come to expect their financial institution will be a good steward of their money. While no industry is perfect, it's for good reason that financial firms are held up as leading the economy in security and security-related innovation.



Source: *ITRC Data Breach Report 2017*

As the data shows, no business or industry segment is immune to hackers. Financial institutions are, not surprisingly, frequent targets of hackers. As Robert Novy, Deputy Assistant Director at the U.S. Secret Service put it: "US financial and payment systems were, and remain, the natural target for much of this criminal activity – for the simple reason, as the bank robber Willie Sutton was once reported to have quipped, 'That's where the money is at.'"[9]

[8] See Appendix B
[9] See *2017 Verizon Data Breach Investigations Report, Appendix B.*

As the data also makes clear, despite the prevalence and frequency of attacks, the financial industry continues to make the necessary investments that have minimized the overall frequency of data breaches within our industry. Cybersecurity is a regular discussion item from the first line operating level all the way up to Executive Management teams and the Board of Directors. For many FSR members, for example, cybersecurity is a discussion item for the full Board and Board Committees on a quarterly basis, if not more often.[10]

More innovation is taking place throughout the payments ecosystem than in arguably any other aspect of financial services. From increasing security and reducing fraud to creating a more friction-free experience for consumers, our industry is committed to building and implementing the systems to maintain our role as consumers' trusted source for payments and managing money. New methods of biometric authentication, cloud-based technology, location-based services, and keystroke behavior patterns will be the norm in the future.

More immediately, tokenization – which replaces sensitive financial information with data that can only be interpreted by a very limited set of parties in the transaction chain, but is of no value if stolen in a data breach – is paving the way for mobile payments to become a widely adopted method of payment consumers can trust. Tokenization, along with biometrics to help in customer authentication, are the key security drivers that brought Apple Pay and other digital wallets to market creating what is, according to many, the most secure payment experience available.[11]

The security technology behind Apple Pay is a good example of how a layered approach – incorporating a variety of technologies – is needed to ensure consumer data is protected. Again, there is no single panacea to preventing fraud and stopping data breaches.

This Discussion Draft, however, is a very positive step forward to filling an important policy void.

[10] See FSR/BITS "Deciphering Cyber for Your Board of Directors." Available at http://www.fsroundtable.org/wp-content/uploads/2017/10/FSR-BITS-Deciphering-Cyber-for-Your-Board-of-Directors-Facilitating-a-Better-Dialogue.pdf

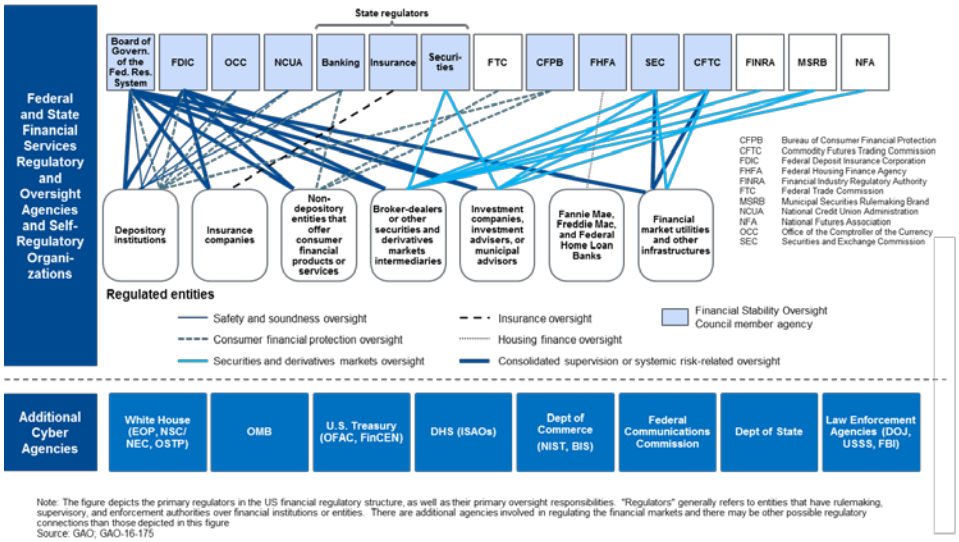
[11] http://mashable.com/2014/10/23/apple-pay-is-more-secure-than-your-credit-and-debit-cards/

Protection of Information

Overview

According to a report published by Homeland Security Research Corp., the financial services cybersecurity market in the United States reached an estimated $9.5 billion in 2016, making it the largest non-government cybersecurity market.[12] Of that number, the top four U.S. banks spent nearly $1.5 billion.[13] In addition, other reports indicate that firms within the financial sector "…spend more on IT security than any other sector, spending three times as much as comparably sized non-financial institutions."[14]

As members of this Subcommittee are well aware, cyber and data protection practices of the financial industry are overseen by nine independent federal regulators, three self-regulatory organizations, the U.S. Department of the Treasury as it sector-specific agency, and every state banking and securities agency. When agencies tasked with cyber-related authorities are added, the list expands even further.



While FSR and its members are actively working to harmonize many of these complexities, our members appreciate the need for robust oversight and regulation of our cybersecurity practices.

All of these obligations stem from a single law, the Gramm-Leach-Bliley Act (Pub.L. 106-102) (GLBA), enacted in 1999. Section 501(b) of Title V of this law directed federal and state regulators with oversight of financial institutions and the FTC to establish

[12] See: http://homelandsecurityresearch.com/2014/10/u-s-banking-financial-services-retail-payment-cybersecurity-market-2015-2020/
[13] See: https://www.forbes.com/sites/stevemorgan/2015/12/13/j-p-morgan-boa-citi-and-wells-spending-1-5-billion-to-battle-cyber-crime/#7204cf13116d
[14] See: https://go.kaspersky.com/rs/802-IJN-240/images/Financial_Survey_Report_eng_final.pdf.

appropriate standards and processes relating to administrative, technical and physical safeguards to protect customer information.

We are not suggesting that all unregulated sectors of the economy be subjected to comparable levels of regulatory burden and oversight, nor would this make sense or even be feasible: Most firms across the economy have minimal or no exposure to consumers' sensitive financial or personal information that would warrant this level of intense cybersecurity oversight. It should also be noted that no government examination agency even exists with the capacity to conduct such oversight of every business in the country.

However, FSR strongly believes Congress needs to act to require firms of all shapes and sizes that handle sensitive information to protect the data, and it should do so by creating a robust, yet flexible and scalable, data security framework.

On the Discussion Draft

The approach detailed in the Discussion Draft strikes the appropriate balance by setting a high bar for data protection, while providing numerous considerations to ensure a small business that processes or maintains little or no personal information is not burdened with the same expectations as a larger entity.

The standards and processes produced as a result of Title V of GLBA provide a useful comparison: GLBA's implementing regulations include a similar set of considerations as the Discussion Draft outlines in section 2(a)(2). These GLBA standards apply to the smallest credit union or community bank and the largest member of FSR. There are no carve-outs for institutions under a certain asset size: Instead – and the rules the financial industry follows on this are explicit – the tools our industry employs to protect customers must be appropriate to the size and complexity of the organization, the nature and scope of its activities, and the sensitivity of the information it handles. These considerations have demonstrated that the most robust cybersecurity expectations can be appropriately tailored to firms that differ dramatically in their data protection needs.

Furthermore, the Discussion Draft refrains from mandating specific technologies. This is a critical point, and speaks to the benefit of legislating a process- and risk-based framework: Picking technological winners and losers in statute is a sure-fire way to suppress innovation and tie the hands of cybersecurity professional seeking to defend their companies against attack. Rigid legal requirements fail to keep up with the dynamic cyber threat environment, forcing companies to focus on compliance rather than building the most effective cyber defenses against criminals.

Notification of Breach of Data Security

Overview

Similar to the existing requirements for financial institutions to protect customer data outlined above, GLBA also requires financial institutions to maintain customer notification programs that would ensure financial firms provide notice to impacted customers when the financial institution itself suffered a breach.

Some non-financial trade groups continue to make the assertion that banks are not required under GLBA to provide notice to consumers of their own data breach. They base this claim on the fact that the bank regulators issued interagency "guidance" on consumer breach notification which, in their estimation, does not amount to a mandate. This is a false assertion, however, as it fails to recognize that guidance is often treated by prudential regulators in the ongoing oversight and examination process as a requirement that is due the same adherence as law or regulation.

As such, before discussing the notice provision of the Discussion Draft, I would like to take this opportunity to explain how financial institutions are, in fact, required to maintain breach incident response programs:

- In 2005, the federal banking agencies jointly issued interagency guidance (interpreting Section 501(b) of GLBA and the Interagency Guidelines) concerning how a financial institution must respond to the unauthorized acquisition or use of customer information.[15]
- This Guidance is a Safety and Soundness standard issued under the federal banking agencies' safety and soundness authority under Section 39 of the Federal Deposit Insurance Act,[16] as well as under Section 501(b) of GLBA.[17]
- Federal banking agencies examine financial institutions for their compliance with the Guidance. In this regard, the Guidance is not treated as a recommendation: It is a Safety and Soundness standard for which compliance is demanded.
- The federal banking agencies may fine or otherwise penalize a financial institution for its failure to comply with the Guidance, by – as an example – issuing Matters Requiring Attention (MRAs). As an illustration, in reference to the notification

[15] 12 C.F.R. pt. 364, App. B (FDIC); 12 C.F.R. pt. 208, App. D-2 and pt 225, App. F (FRB); 12 C.F.R. pt. 30, App. B (OCC). *See also* 70 Fed. Reg. 15,736 (Mar. 29, 2005).
[16] *See* https://www.fdic.gov/regulations/laws/rules/1000-4100.html
[17] *See, E.G.,* 12 C.F.R. 30.2.

Guidance, the Office of the Comptroller of the Currency (OCC) states: *The OCC may treat a bank's failure to implement the final guidance as a violation of the Security Guidelines that are enforceable under the procedures set forth in 12 USC 1831p-1, or as an unsafe and unsound practice under 12 USC 1818.*[18]

- If the financial institution determines misuse of the information "has occurred or is reasonably possible," the financial institution "should notify the affected customer as soon as possible." The Guidance uses the term "should" to express a financial institution's obligation or duty to notify, as opposed to a recommendation. That is, the Guidance *requires* notice in accordance with its standards, as opposed to only recommending notice.
- The Guidance states that financial institutions have "an affirmative duty" to protect customer information from unauthorized access or use.[19] In this regard, the Guidance clarifies that **"[n]otifying customers of a security incident involving the unauthorized access or use of the customer's information in accordance with the standard set forth [in the Guidance] is a key part of that duty."** Again: Notice to customers in accordance with the Guidance is an "affirmative duty."
- The Guidance clarifies that "[w]hen customer notification is warranted, an institution may not forgo notifying its customers of an incident because the institution believes that it may be potentially embarrassed or inconvenienced by doing so."[20]
- Notice obligations extend equally with respect to incidents involving customer information at a financial institution's service provider. Specifically, the Guidance provides that where unauthorized access to customer information occurs at a financial institution's service provider, "it is the responsibility of the financial institution to notify the institution's customers and regulator."[21] Banking agencies further require financial institutions to ensure their service provider contracts address procedures for notifying the institution of security breaches that pose risk to consumers. *Once more: Notice is a responsibility and a duty, not a recommendation.*

Not only do FSR members take the protection of data very seriously, they also prioritize customer service and communication – of both good news and bad. Suggesting these requirements of GLBA are in some way optional is misinformed and misguided.

---

[18] http://www.occ.treas.gov/news-issuances/bulletins/2005/bulletin-2005-13.html
[19] See, e.g., 12 C.F.R. pt. 30, App. B, Supp. A, III.
[20] *See, e.g.*, 12 C.F.R. pt. 30, App. B, Supp. A, III.
[21] *See, e.g.*, 12 C.F.R. pt. 30, App. B, Supp. A, II(A)(2).

On the Discussion Draft

- FSR strongly supports a risk-based trigger, which will help ensure consumers are notified when they are actually at risk from a breach. Over-notification leads to de-sensitization, which can cause consumers to ignore warnings and the need to act that a legitimate risk-inducing data breach notice can provide. The Discussion Draft calls for consumers to be notified when a breach is reasonably likely to result in "identity theft, fraud, or economic loss." While "economic loss" is an extremely broad term that should be clarified, overall this risk-based approach is the appropriate construction.
- On the issue of the timing of notifications, as discussed in the Subcommittee's hearing on February 14, 2018, the key question for policymakers is when legislation should specify the proverbial "clock starts ticking." The Discussion Draft contemplates that the clock starts ticking after the covered entity completes its preliminary investigation required under Sec. 4(a). This is the correct approach: Premature notification – i.e., notice being provided *before* a covered entity has ascertained a fuller picture of the breach, determined whether or not the breach compromised personal information, the loss of which could result in identity theft, fraud or economic loss, and taken initial steps to secure their compromised systems – may result in false alarms. The Discussion Draft sets a practical and balanced standard that will contribute to accurate notification to impacted consumers.
- The Discussion Draft states consumers are to be notified "immediately…without unreasonable delay." The introduction of an "immediate" timeframe for notification is, perhaps, without precedent. Most state laws have adopted a variation on one of two themes: Either "in the most expedient time possible and without unreasonable delay" or simply "without unreasonable delay."[22] The Committee should consider any of these similar concepts that can ensure consumers are notified as soon as possible while not creating unnecessary or unwarranted alarm.

Enforcement and Preemption

- The Discussion Draft provides for enforcement over financial institutions by the federal banking regulators, and the Federal Trade Commission (FTC) and state Attorneys General for other sectors that do not have functional oversight. We believe this is an appropriate approach that does not duplicate the ongoing,

[22] See Appendix C.

regular enforcement activities of federal bank examiners. *This is an important distinction: Financial institutions have examiners, empowered with significant enforcement tools, overseeing their information security and breach notice responsibilities in an ongoing capacity. Examiners have similar oversight authority over technology service providers to those financial institutions. No other sector subject to this legislation has equivalent oversight and enforcement.*

- Few issues are as ripe for federal legislative action as data security. FSR and others have over the years described the patchwork of conflicting state laws, which illustrates the need for Congress to act in a way that sets one strong, uniform national standard. To echo an important sentiment: Whether or not a person's data is protected should not depend on where they live. That is why FSR firmly believes Congress must enact a robust yet flexible framework for the protection of sensitive information, a threshold achieved by the Discussion Draft.

Conclusion

Data breach and payment security issues are fundamentally about protecting consumers. Every American business that handles sensitive financial information should have an innate motivation to protect it, if for no other reason than maintaining the trust and continued business of their customers.

I would like to conclude by revisiting the key questions I posed at the outset:

What companies have my data? The answer is, more than any of us probably realize. Which is all the more reason for Congress to act to ensure that no matter where the data resides, it is protected.

How are those companies protecting it? Today, they are only required to protect it if the small number of state security laws are applicable to their business. Again, where a person lives should not dictate whether or not their data is required to be protected. That said, setting the appropriately high standard and framework for protection is critical, as is not making specific technology mandates. The Discussion Draft strikes the right balance.

If they lose my data will I found out, and when? Customers must be made aware of a breach when they are at risk, and that notification must happen quickly. That said, the company that suffered the breach needs a reasonable amount of time to ascertain what happened, identify impacted customers, involve law enforcement and secure their systems. This should not be an excuse to drag out notification, however.

What is the federal government's role in keeping my data secure? The sectoral approach adopted by the U.S. has addressed data protection for two of the most sensitive industries: Financial services and healthcare. For the financial sector, that has evolved into comprehensive rules and regulations, enforced by numerous agencies through robust on-site examinations. However, the proliferation and importance of data to every sector of the economy has highlighted the need for the federal government to take steps to keep it secure. Both bills that are the topics of today's hearing take important steps to address these challenges.

Thank you for inviting me to testify. I look forward to your questions.

Appendix A

Federal Laws & Regulations Related to Financial Institutions' Obtaining Social Security Numbers

Statute & Regulation	Social Security Number Requirement	Retention/Disposal Provisions
A. BSA/AML		
Customer Identification Program *31 C.F.R. § 1020.220*	**Prior to opening an account**, the bank/thrift/credit union must, at a minimum, obtain the customer's name, date of birth, address (residential or business), and an **identification number** (can be taxpayer identification number).	The bank must retain identifying information for **five years after the account is closed**.
Purchases of bank checks and drafts, cashier's checks, money orders and traveler's checks *31 C.F.R. § 1010.415*	**No financial institution may issue or sell a bank check or draft, cashier's check, money order or traveler's check for $3,000 or more in currency unless it maintains records of the following information,** which must be obtained for each issuance or sale of one or more of these instruments to any individual purchaser which involves currency in amounts of $3,000-$10,000 inclusive: **If the purchaser does not have a deposit account with the financial institution:** (A) The name and address of the purchaser; (B) The **social security number** of the purchaser, or if the purchaser is an alien and does not have a social security number, the alien identification number; (C) The date of birth of the purchaser; (D) The date of purchase; (E) The type(s) of instrument(s) purchased; (F) The serial number(s) of the instrument(s) purchased; and (G) The amount in dollars of each of the instrument(s) purchased.	Records required to be kept shall be retained by the financial institution for a period of **five years** and shall be made available to the Secretary upon request at any time.
Beneficial Ownership *31 C.F.R. § 1010.230* *(effective May 11, 2018)*	Financial institutions are required to obtain, verify, and record the identities of the beneficial owners of legal entity customers. As with CIP for individual customers, covered financial institutions must collect from the legal entity customer the name, date of birth, address, and **social security number** or other government identification number (passport number or other similar information in the case of foreign persons) for individuals who own 25% or more of the equity interest of the legal entity (if any), and an individual with significant responsibility to control/manage the legal entity at the time a new account is opened.	A financial institution must retain the records for five years after the date the account is closed.
B. Consumer Financial Products and Services		
Application for a residential mortgage loan (Truth in Lending Act)	For residential mortgage transactions, an application consists of the submission of the consumer's name, the consumer's income, the consumer's **social security number** to obtain a credit report, the property address, an estimate of the value of the property, and the mortgage loan amount sought.	A creditor shall retain evidence of compliance for **two years** after the date disclosures are required to be made or

12 C.F.R. §§ 1026.3(a)(3)(ii); 1026.25		action is required to be taken.
Electronic Fund Transfer Act – Error Notice *12 C.F.R. §§ 1005.11 and 1005.13*	A financial institution shall comply with the requirements of this section with respect to any oral or written notice of error from the consumer that: (i) Is received by the institution no later than 60 days after the institution sends the periodic statement or provides the passbook documentation, on which the alleged error is first reflected; (ii) Enables the institution to identify the consumer's name and account number; and(iii) Indicates why the consumer believes an error exists and includes to the extent possible the type, date, and amount of the error, except for requests described in paragraph (a)(1)(vii) of this section. ***Content of error notice.*** The notice of error is effective even if it does not contain the consumer's account number, so long as the financial institution is able to identify the account in question. For example, the consumer could provide a Social Security number or other unique means of identification.	Any person subject to the Act and this part shall retain evidence of compliance with the requirements imposed by the Act and this part for a period of not less than **two years** from the date disclosures are required to be made or action is required to be taken.
C. Privacy/Information Security		
Privacy of Financial Information *12 C.F.R. pt. 332*	**Nonpublic personally identifiable information includes any information a** consumer provides to you to obtain a financial product or service from you. The regulation: (1) Requires a financial institution to provide notice to customers about its privacy policies and practices; (2) Describes the conditions under which a financial institution may disclose nonpublic personal information about consumers to nonaffiliated third parties; and (3) Provides a method for consumers to prevent a financial institution from disclosing that information to most nonaffiliated third parties by "opting out" of that disclosure, subject to exceptions.	No specific recordkeeping requirement.
Interagency Guidelines Establishing Information Security Standards *12 C.F.R. pt. 364, App. B (and corresponding regs)*	An institution must protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer. Substantial harm or inconvenience is most likely to result from improper access to **sensitive customer information, which includes SSN,** because this type of information is most likely to be misused, as in the commission of identity theft. **Notice to Regulator:** The institution's response program must include procedures for notifying its primary federal regulatory as soon as possible when the institution becomes aware of an incident involving unauthorized access to or uses of **sensitive customer information.**	An institution's information security program must ensure the proper disposal of customer information and consumer information.

	Notice to Consumer: When a financial institution becomes aware of an incident of unauthorized access to **sensitive customer information**, the institution should conduct a reasonable investigation to promptly determine the likelihood that the information has been or will be misused. If the institution determines that misuse of its information about a customer has occurred or is reasonably possible, it should notify the affected customer as soon as possible. Customer notice may be delayed if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and provides the institution with a written request for the delay. However, the institution should notify its customers as soon as notification will no longer interfere with the investigation.	
D. Identity Theft/Consumer Reports		
Red Flags Rule *12 C.F.R. pt. 334, App. J (and corresponding regs)*	Requires financial institutions and creditors to develop and provide for the continued administration of a written Program to detect, prevent, and mitigate identity theft in connection with the opening of a covered account or any existing covered account. Each financial institution or creditor may consider incorporating into its Program, whether singly or in combination, Red Flags from the following illustrative examples in connection with covered accounts: Suspicious personal identifying information includes: • Social security number has not been issued or is listed on the Social Security Administration's Death Master File • Lack of correlation between the SSN range and date of birth • The SSN provided is the same as that submitted by other persons opening an account or other customers.	
Duties of Consumer Reporting Agencies Regarding Identity Theft *12 C.F.R. § 1022.123*	**Consumer reporting agencies shall develop and implement reasonable requirements for what information consumers shall provide to constitute proof of identity** where the consumer asserts a good-faith belief that have been a victim of identity fraud or a related crime. **Examples of information** that might constitute reasonable information requirements for proof of identity are provided for illustrative purposes only: *Consumer file match.* The identification information of the consumer including his or her full name (first, middle initial, last, suffix), any other or previously used names, current and/or recent full address (street number and name, apt. no., city, state, and zip code), full nine digits of **Social Security number**, and/or date of birth.	
Disclosure by CRA of Consumer File to	Every consumer reporting agency shall, upon request, clearly and accurately disclose to the consumer **all information in the consumer's file** at the time of the request, except that if the	

Consumer; Free Annual Report; *15 U.S.C. §§ 1681g, 1681h, 1681j(a); 12 C.F.R. pt. 1022, subpart N.*	consumer to whom the file relates requests that the first five digits of the SSN not be included, and the reporting agency has adequate proof of the identity of the requester, the reporting agency shall so truncate the disclosure. A CRA shall require, as a condition of making that disclosure, that the consumer furnish **proper identification**. <u>Free Annual Reports:</u> There is a centralized source for requesting annual file disclosures from nationwide CRAs which collects only as much **personally identifiable information** as is reasonably necessary to properly identify the consumer and to process the transaction requested by the consumer. Any **personally identifiable information** collected from consumers as a result of a request for annual file disclosure, or other disclosure required by the FCRA, made through the centralized source, may be used or disclosed by the centralized source or a nationwide consumer reporting agency only: (1) To provide the annual file disclosure or other disclosure required under the FCRA requested by the consumer; (2) To process a transaction requested by the consumer at the same time as a request for annual file disclosure or other disclosure; (3) To comply with applicable legal requirements, including those imposed by the FCRA and this part; and (4) To update personally identifiable information already maintained by the nationwide consumer reporting agency for the purpose of providing consumer reports, provided that the nationwide consumer reporting agency uses and discloses the updated personally identifiable information subject to the same restrictions that would apply, under any applicable provision of law or regulation, to the information updated or replaced.	

Appendix B

January 4, 2018

The Honorable Greg Walden
Chairman
House Energy & Commerce Committee
2125 Rayburn House Office Building
Washington, DC 20515

The Honorable Bob Latta
Chairman
Subcommittee on Digital Commerce and Consumer Protection
2125 Rayburn House Office Building
Washington, DC 20515

Dear Chairman Walden and Chairman Latta:

The undersigned organizations, representing companies across the American economy, take the stewardship and protection of customers' personal information very seriously. That is why we support federal legislation to protect personal information and, in the event of a data breach that could result in identity theft or other financial harm, ensure consumers are notified in a timely manner.

We believe that Congress should enact legislation encompassing the following elements:

- A flexible, scalable standard for data protection that factors in (1) the size and complexity of an organization, (2) the cost of available tools to secure data, and (3) the sensitivity of the personal information an organization holds, as well as guarantees that small organizations are not burdened by excessive requirements.

- A notification regime requiring timely notice to impacted consumers, law enforcement, and applicable regulators when there is a reasonable risk that a breach of unencrypted personal information exposes consumers to identity theft or other financial harm.

- Consistent, exclusive enforcement of the new national standard by the Federal Trade Commission (FTC) and state Attorneys General, other than for entities subject to state insurance regulation or who comply with the Gramm-Leach-Bliley Act or the Health Insurance Portability and Accountability Act of 1996/HITECH Act. For entities under its jurisdiction, the FTC should have the authority to impose penalties for violations of the new law.

- Clear preemption of the existing patchwork of often conflicting and contradictory state laws.

Data security impacts every sector of the economy. We therefore look forward to working with you and your colleagues to ensure that all sectors employ sound data security and alert consumers when a breach may result in identity theft or other financial harm.

Sincerely,

ACT | The App Association

American Bankers Association

American Council of Life Insurers

American Insurance Association

American Land Title Association

BSA | The Software Alliance

Consumer Bankers Association

Credit Union National Association

CTIA

Electronic Transactions Association

Financial Services Roundtable

Independent Community Bankers of America

Independent Insurance Agents and Brokers of America

Internet Commerce Coalition

National Association of Federally-Insured Credit Unions

National Association of Mutual Insurance Companies

National Business Coalition on E-Commerce & Privacy

Property Casualty Insurers Association of America

Reinsurance Association of America

Retail Industry Leaders Association

TechNet

Twenty-First Century Privacy Coalition

USTelecom

Appendix C

State Data Breach Notification Laws: Timing of Consumer Notice

STATE	TIMING
ALASKA	Must be made in the most expeditious time possible and without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
ARIZONA	Must be made in the most expeditious time possible and without unreasonable delay consistent with any measures to determine the scope of the breach, to identify residents affected, and to restore the reasonable integrity of the system.
ARKANSAS	Must be made in the most expeditious time possible and without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
CALIFORNIA	Must be made in the most expeditious time possible and without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
COLORADO	Must be made in the most expeditious time possible and without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
CONNECTICUT	Must be made in the most expeditious time possible and without unreasonable delay consistent with any measures to determine the scope of the breach, to identify those affected, or to restore the reasonable integrity of the system.
DELAWARE	Must be made in the most expedient time possible and without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
DISTRICT OF COLUMBIA	Must be made in the most expedient time possible and without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
FLORIDA	Must be made as expeditiously as practicable and without unreasonable delay but no later than 30 days after the determination of breach, consistent with time necessary to determine the scope of the breach, identify those affected, and restore the reasonable integrity of the system.
GEORGIA	Must be made in the most expedient time possible and without unreasonable delay consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the system.
GUAM	Must be made without unreasonable delay consistent with any measures necessary to determine the scope of the breach and to restore the reasonable integrity of the system
HAWAII	Must be made without any unreasonable delay consistent with any measures to determine contact info, the scope of the breach, and to restore the reasonable integrity, security, and confidentiality of the system.
IDAHO	Must be made in most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach, identify the resident affected, and restore the reasonable integrity of the system.

ILLINOIS	Must be made in the most expedient time possible and without unreasonable delay, consistent with any measures to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the system.
INDIANA	Must be made without unreasonable delay, consistent with necessary measures to restore the integrity of the system or necessary to discover the scope of the breach.
IOWA	Must be made in most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach, sufficiently determine contact info for the residents affect, and restore the reasonable integrity of the system.
KANSAS	Must be made in most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.
KENTUCKY	Must be made in most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.
LOUISIANA	Must be made in most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach, prevent further disclosures, and restore the reasonable integrity of the system.
MAINE	Must be made in most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach, identify the individuals affected, and restore the reasonable integrity of the system.
MARYLAND	Must be made as soon as reasonably practicable after the investigation but after given notice to the Attorney General, consistent with measures to determine scope of the breach, identify individuals affected or restore the integrity of the systems.
MASSACHUSETTS	Must be made as soon as practicable and without unreasonable delay.
MICHIGAN	Must be made without unreasonable delay, consistent any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.
MINNESOTA	Must be made in most expedient time possible and without unreasonable delay, consistent with any measures necessary to determine the scope of the breach, identify those affected, and restore the reasonable integrity of the system.
MISSISSIPPI	Must be made without unreasonable delay, subject to the completion of an investigation to determine the nature and scope of the breach or to restore the reasonable integrity of the system.
MISSOURI	Must be made without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity, security, and confidentiality of the system.
MONTANA	Must be made without unreasonable delay, consistent with any measures necessary to determine the scope of the breach and restore the reasonable integrity of the system.
NEBRASKA	Must be made as soon as possible and without unreasonable delay, consistent with any measures necessary to determine the scope and restore the reasonable integrity of the system.

NEVADA	Must be made in the most expedient time possible and without unreasonable delay, consistent with any measures to determine the scope of the breach and restore the reasonable integrity of the system.
NEW HAMPSHIRE	Must be made as soon as possible.
NEW JERSEY	Must be made in the most expedient time possible and without unreasonably delay and consistent with any measures necessary to determine the scope of the breach and to restore the integrity of the system.
NEW MEXICO	Must be made in the most expedient time possible, but no later than 45 calendar days following discovery of the breach, subject to the delay provision discussed below.
NEW YORK	Must be made in the most expedient time possible and without unreasonable delay and consistent with any measures necessary to determine the scope of the breach and to restore the integrity of the system.
NORTH CAROLINA	Must be made without unreasonable delay taking any necessary measures to determine sufficient contact info, determine the scope of the breach and to restore the reasonably integrity, security, and confidentiality of the system.
NORTH DAKOTA	Must be made in the most expedient time possible and without unreasonable delay and consistent with any measures necessary to determine the scope of the breach and to restore the integrity of the system.
OHIO	Must be made in the most expedient time possible but not later than 45 days following its discovery of the breach consistent with any measures necessary to determine the scope of the breach, include which consumers' info was accessed or acquired, and to restore the reasonable integrity of the system.
OKLAHOMA	Must be made in the most expedient time possible without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
OREGON	Must be made in the most expeditious time possible and without unreasonable delay and consistent with any measures necessary to determine sufficient contact info, determine the scope of the breach, or restore the reasonable integrity, security, and confidentiality of the data.
PENNSYLVANIA	Must be made without unreasonable delay taking any necessary measures to determine the scope of the breach and to reasonable restore the integrity of the system.
PUERTO RICO	As expeditiously as possible consistent with any measures to restore the security of the system.
RHODE ISLAND	Must be made in the most expedient time possible but no later than 45 days after confirmation of the breach and the ability to ascertain information that must be included in the consumer notice.
SOUTH CAROLINA	Must be made in the most expedient time possible without any unreasonably delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
TENNESSEE	Must be made immediately but no later than 45 days from discovery of the breach.
TEXAS	Must be made as quickly as possible, except as necessary to determine the scope of the breach and restore the reasonable integrity of the system.
UTAH	Must be made in the most expedient time possible without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.

VERMONT	Must be made in the most expedient time possible and without unreasonable delay but not later than 45 days after discovery and consistent with any measures to determine the scope of the breach and to restore the reasonable integrity, security, and confidentiality of the system.
VIRGIN ISLANDS	Must be made in the most expedient time possible and without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
VIRGINIA	Must be made without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
WASHINGTON	Must be made in the most expedient time possible without unreasonable delay but no more than 45 calendar days after the breach was discovered, consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
WEST VIRGINIA	Must be made in the most expedient time possible and without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.
WISCONSIN	Must be made within a reasonable time not to exceed 45 days, subject to law enforcement delay
WYOMING	Must be made in the most expedient time possible and without unreasonable delay consistent with any measures to determine the scope of the breach and to restore the reasonable integrity of the system.