

DATA SECURITY: VULNERABILITIES AND OPPORTUNITIES FOR IMPROVEMENT

HEARING BEFORE THE SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT OF THE COMMITTEE ON FINANCIAL SERVICES U.S. HOUSE OF REPRESENTATIVES ONE HUNDRED FIFTEENTH CONGRESS FIRST SESSION

NOVEMBER 1, 2017

Printed for the use of the Committee on Financial Services

Serial No. 115-52



U.S. GOVERNMENT PUBLISHING OFFICE

30-771 PDF

WASHINGTON : 2018

HOUSE COMMITTEE ON FINANCIAL SERVICES

JEB HENSARLING, Texas, *Chairman*

PATRICK T. MCHENRY, North Carolina,
Vice Chairman

PETER T. KING, New York
EDWARD R. ROYCE, California
FRANK D. LUCAS, Oklahoma
STEVAN PEARCE, New Mexico
BILL POSEY, Florida
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
SEAN P. DUFFY, Wisconsin
STEVE STIVERS, Ohio
RANDY HULTGREN, Illinois
DENNIS A. ROSS, Florida
ROBERT PITTENGER, North Carolina
ANN WAGNER, Missouri
ANDY BARR, Kentucky
KEITH J. ROTHFUS, Pennsylvania
LUKE MESSER, Indiana
SCOTT TIPTON, Colorado
ROGER WILLIAMS, Texas
BRUCE POLQUIN, Maine
MIA LOVE, Utah
FRENCH HILL, Arkansas
TOM EMMER, Minnesota
LEE M. ZELDIN, New York
DAVID A. TROTT, Michigan
BARRY LOUDERMILK, Georgia
ALEXANDER X. MOONEY, West Virginia
THOMAS MacARTHUR, New Jersey
WARREN DAVIDSON, Ohio
TED BUDD, North Carolina
DAVID KUSTOFF, Tennessee
CLAUDIA TENNEY, New York
TREY HOLLINGSWORTH, Indiana

MAXINE WATERS, California, *Ranking
Member*

CAROLYN B. MALONEY, New York
NYDIA M. VELÁZQUEZ, New York
BRAD SHERMAN, California
GREGORY W. MEEKS, New York
MICHAEL E. CAPUANO, Massachusetts
WM. LACY CLAY, Missouri
STEPHEN F. LYNCH, Massachusetts
DAVID SCOTT, Georgia
AL GREEN, Texas
EMANUEL CLEAVER, Missouri
GWEN MOORE, Wisconsin
KEITH ELLISON, Minnesota
ED PERLMUTTER, Colorado
JAMES A. HIMES, Connecticut
BILL FOSTER, Illinois
DANIEL T. KILDEE, Michigan
JOHN K. DELANEY, Maryland
KYRSTEN SINEMA, Arizona
JOYCE BEATTY, Ohio
DENNY HECK, Washington
JUAN VARGAS, California
JOSH GOTTHEIMER, New Jersey
VICENTE GONZALEZ, Texas
CHARLIE CRIST, Florida
RUBEN KIHUEN, Nevada

KIRSTEN SUTTON MORK, *Staff Director*

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

BLAINE LUETKEMEYER, Missouri, *Chairman*

KEITH J. ROTHFUS, Pennsylvania, *Vice
Chairman*

EDWARD R. ROYCE, California

FRANK D. LUCAS, Oklahoma

BILL POSEY, Florida

DENNIS A. ROSS, Florida

ROBERT PITTENGER, North Carolina

ANDY BARR, Kentucky

SCOTT TIPTON, Colorado

ROGER WILLIAMS, Texas

MIA LOVE, Utah

DAVID A. TROTT, Michigan

BARRY LOUDERMILK, Georgia

DAVID KUSTOFF, Tennessee

CLAUDIA TENNEY, New York

WM. LACY CLAY, Missouri, *Ranking
Member*

CAROLYN B. MALONEY, New York

GREGORY W. MEEKS, New York

DAVID SCOTT, Georgia

NYDIA M. VELÁZQUEZ, New York

AL GREEN, Texas

KEITH ELLISON, Minnesota

MICHAEL E. CAPUANO, Massachusetts

DENNY HECK, Washington

GWEN MOORE, Wisconsin

CHARLIE CRIST, Florida

CONTENTS

	Page
Hearing held on:	
November 1, 2017	1
Appendix:	
November 1, 2017	35

WITNESSES

WEDNESDAY, NOVEMBER 1, 2017

Bentsen, Hon. Kenneth, Jr., President and Chief Executive Officer, Securities Industry and Financial Markets Association	3
Mennenoh, Daniel, ITP, NTP, President, H.B. Wilkinson Title Company, on behalf of the American Land Title Association	5
Mierzwinski, Edmund, Consumer Program Director, U.S. Public Interest Research Group	6
Schwartz, Debra, President and Chief Executive Officer, Mission Federal Credit Union, on behalf of the National Association of Federally-Insured Credit Unions	8

APPENDIX

Prepared statements:	
Bentsen, Hon. Kenneth, Jr.	36
Mennenoh, Daniel	50
Mierzwinski, Edmund	61
Schwartz, Debra	78

ADDITIONAL MATERIAL SUBMITTED FOR THE RECORD

Luetkemeyer, Hon. Blaine:	
Written statement of the Food Marketing Institute	105
Written statement of the Independent Community Bankers of America	107
Written statement of the American Bankers Association, the Consumer Bankers Association, the Credit Union National Association, the Financial Services Roundtable, the Independent Community Bankers of America, the National Association of Federally-Insured Credit Unions, and the The Clearing House	109

DATA SECURITY: VULNERABILITIES AND OPPORTUNITIES FOR IMPROVEMENT

Wednesday, November 1, 2017

U.S. HOUSE OF REPRESENTATIVES,
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS
AND CONSUMER CREDIT,
COMMITTEE ON FINANCIAL SERVICES,
Washington, D.C.

The subcommittee met, pursuant to notice, at 2:02 p.m., in room 2128, Rayburn House Office Building, Hon. Blaine Luetkemeyer [chairman of the subcommittee] presiding.

Present: Representatives Luetkemeyer, Rothfus, Royce, Lucas, Ross, Pittenger, Barr, Tipton, Williams, Love, Trott, Loudermilk, Kustoff, Tenney, Clay, Maloney, Scott, and Crist.

Chairman LUETKEMEYER. The committee will come to order.

Without objection, the chair is authorized to declare a recess of the committee at any time.

This hearing is entitled "Data Security: Vulnerabilities and Opportunities for Improvement."

Before we begin, I would like to thank the witnesses for appearing today. We appreciate your participation and look forward to a productive discussion.

I now recognize myself for 3 minutes for purposes of delivering an opening statement.

More than 15 million Americans were victims of cyber fraud or identity theft last year. The number of those impacted in 2017 could be significantly more, depending on the damage caused by the Equifax breach. While data security has been a hot topic since that breach, Equifax isn't where the problem started, and if we don't act, it isn't where the problem will end.

Year after year, consumers deal with compromised personally identifiable information resulting from breaches in financial companies, retailers, insurance providers, and even the Federal Government. The list goes on and on.

This type of fraud can strike at any point, leaving no consumer immune to its effects. Financial firms face attempted breaches every single day, sometimes hundreds of attempts a day. Each attack seems to be more dangerous and more advanced than the last, and while the good guys have to be right every time, the bad guys only have to be right once.

Data security has turned into a crisis, and the American people deserve better. As in any crisis, every aspect of data security should be examined. That includes having an honest conversation

about the regulatory regime governing these breaches. The question is, does it adequately safeguard consumer data? Does it provide flexibility for companies to innovate, or do they spend too much time and energy trying to comply with State and Federal requirements?

We need to discuss how data security liability is assessed and which entity has a duty to report a breach to the public and in what timeframe such a disclosure should be required. We cannot tolerate a system that is unnecessarily complicated or offers slow resolution for customers and consumers. We need to instead work collaboratively to reduce red tape, create a more prompt notification standard, and foster harmonization among Federal and State agencies charged with data security regulation.

Today's hearing offers an opportunity to look at data security vulnerabilities through a wider lens. Our witnesses represent a number of different industries that offer unique perspectives and ideas on how to improve the system for the most important people in this conversation: their customers and our constituents.

While today's hearing does not focus on a specific bill, I want to be clear that it is my intention to produce data security reform legislation. This conversation and many others our members have had and will continue to have with their constituents will inform our actions and drive our policy.

I want to again thank our witnesses for being here today. We look forward to your testimony.

The chair now recognizes the gentleman from Missouri, Mr. Clay, the ranking member of the subcommittee, for 5 minutes for an opening statement.

Mr. CLAY. Thank you, Mr. Chairman. Thank you for holding this hearing as well as all of the witnesses who are here today. I will forego an opening statement in order to hear from our witnesses. I yield back.

Chairman LUETKEMEYER. The gentleman yields back.

With that, we go to the gentleman from Pennsylvania, the vice chair of the subcommittee, Mr. Rothfus, for 2 minutes for an opening statement.

Mr. ROTHFUS. Thank you, Mr. Chairman. I would like to thank the chairman for holding today's hearing on data security. As the recent Equifax data breach reminded us, cybercrime is a constant and growing threat. But the Equifax incident, though terrible and expansive as it was, was just the latest in a string of major cybercrimes that have compromised our private information and put us all at risk.

I am deeply concerned that bad actors, State-sponsored or otherwise, continue to relentlessly target our financial system, retailers, and the physical and digital infrastructure that allow our society to function. Cybercrime is a national security threat and a danger to our economy. It hurts millions of Americans, and it undermines the trust needed to conduct business in the 21st century.

This committee has an important role in helping to address this growing threat. I am looking forward to hearing from our witnesses about how we can improve our current system for addressing and preventing cybercrime. Clearly, there is room for improvement as we seek to ensure that firms take the steps needed to protect pri-

vate data, properly and promptly notify law enforcement and customers, and quickly move to close vulnerabilities and make victims whole.

Many of my constituents contacted my office after the Equifax breach to seek help and express their frustrations. Families, students, small business owners, and retirees are concerned about what they are seeing and they want us to take steps to protect them.

Again, I look forward to today's discussion, and I hope that it can form the basis for bipartisan collaboration on this important issue.

I yield back.

Chairman LUETKEMEYER. The gentleman yields back.

With that, today, we welcome the testimony of the Honorable Ken Bentsen, president and chief executive officer, Securities Industry and Financial Markets Association; Mr. Daniel Mennenoh, president, H.B. Wilkinson Title Company, on behalf of the American Land Title Association; Ms. Debra Schwartz, president and CEO, Mission Federally-Insured Credit Union, on behalf of the National Association of Federal Credit Unions; and Mr. Edmund Mierzwinski, consumer program director, U.S. Public Interest Research Group.

Each of the witnesses will now be recognized for 5 minutes to give an oral presentation of their testimony.

Without objection, each of your written statements will be made part of the record.

Just a brief tutorial on the lighting system for those of you who haven't been here before. Green means go. The yellow light lights up, that means you have a minute to wrap up. Red means that we need to stop and go on to the next question/answer session.

With that, Mr. Bentsen, you are recognized for 5 minutes.

STATEMENT OF THE HONORABLE KENNETH BENTSEN, JR.

Mr. BENTSEN. Thank you, Chairman Luetkemeyer and Ranking Member Clay and members of the subcommittee, for giving me an opportunity to testify today on the important topics of cybersecurity and data protection.

SIFMA represents hundreds of banks, broker-dealers, and asset managers who are dedicated to protecting their systems and, more importantly, their clients' data from cyber attacks. There is likely no greater threat to financial stability than a large-scale cyber event. The financial services sector has invested tremendous monetary and human resources to develop and implement cyber defense and recovery mechanisms, and we welcome the opportunity to discuss the progress we have made today.

Cybercrime is now a bigger criminal enterprise than the global narcotics trade. While data breaches of customer information dominate headlines and are rightfully a top priority for policymakers in the industry, a major cyber attack on critical financial market infrastructure or one that destroys records or financial data are also risks with a potentially far larger impact on the economy.

It is important to recognize that no single sector, not the Federal Government nor any individual firm, has the resources to protect markets from these threats on their own. It is critical that we establish and maintain a robust partnership between industry and

government to mitigate cyber threats and their impact. The industry's resiliency will not be fully effective without the government's help and vice versa.

The answer cannot exclusively be more regulation. However, over the past few years, regulators in the U.S. and around the world have proposed or finalized over 30 new cyber rules applicable to the financial services industry. While regulations can help raise expectations and define strong standards for market participants, the volume of regulations has resulted in requirements which are sometimes duplicative and conflicting. Some of our members are subject to as many as 13 different Federal regulatory mandates in addition to State mandates.

Turning to the threat we collectively face, I would like to highlight that every public and private sector institution which holds sensitive information can and, indeed, will be a target of malicious actors. Working with our members along with our sister trade associations, SIFMA has identified a number of best practices for protection of sensitive data in the financial services sector. These practices draw on the experience of our member firms and their own policies and procedures as well as industry standards, such as the NIST framework.

Data protection begins with firms taking a risk-based look at the information they collect, and deciding if they have a business or regulatory purpose that requires them to hold this information. If sensitive information like a social security number is not directly relevant and necessary, firms should refrain from holding it. Once firms have collected sensitive data, they should ensure that they have controls in place to protect it while it is being used and stored. That includes ensuring that access to sensitive data is restricted only to authorized users who need it to perform their jobs. Firms should also work to reduce the risk by destroying sensitive data once it is no longer needed.

As a highly regulated sector, our members also provide a tremendous amount of sensitive information to regulators in accord with their supervisory mandates, and given the ever-increasing risks, our sector is engaged in an important dialog with our government partners to ensure and enhance protections across the board.

I would also like to spend a minute or so to focus on one particular important data protection challenge currently on the minds of many. As the Securities and Exchange Commission and the SROs move forward with the development of a Consolidated Audit Trail, it is critical that the CAT not introduce new data protection risk. Once complete, the CAT will be the world's largest data repository for securities transactions and one of the largest databases of any type. Each day, the system will ingest 58 billion records and maintain the data on over 100 million customer accounts.

The current plan raises serious concerns around data protection and the ability to confidently secure the critical information it will contain. The CAT design requires firms to provide a significant amount of sensitive customer information, including names, social security numbers, and addresses. All this information will be held in a single database, creating a high-value target and bad actors will undoubtedly try to find the weakest link to gain access.

While this concern existed well before the recent breaches at Equifax or EDGAR, many stakeholders have grown even more skeptical that the CAT, as currently designed, will be able to protect the massive amount of sensitive PII it will contain.

Importantly, just as the industry should and does consider whether sensitive information needs to be collected and retained for a particular purpose, so too does the case need to be made that PII is required to be collected and reside in the CAT for effective surveillance by more than 3,000 users among 22 different SROs in the SEC.

Along this line, we would urge Congress to consider among other possible actions amending the Market Data Protection Act to ensure the SROs who designed and built the CAT have appropriate risk controls in place before the CAT goes live.

In conclusion, effective cybersecurity will be in a state of discussion and improvement for years to come. That security is a combination of activities that relies on strong defenses, information sharing, mitigation, and recovery planning. It can only be accomplished through constructive dialog and engagement among the private sector, policymakers, and regulators. Much work has been done, but as my written testimony lays out, there is much more work to do. SIFMA's members stand ready to do their part, and I look forward to answering your questions.

[The prepared statement of Mr. Bentsen can be found on page 36 of the appendix.]

Chairman LUTKEMEYER. Thank you, Mr. Bentsen.

Mr. Mennenoh, you are recognized for 5 minutes.

STATEMENT OF DANIEL MENNENOH

Mr. MENNENOH. Thank you.

Chairman Luetkemeyer, Ranking Member Clay, and members of the subcommittee, I appreciate the opportunity to discuss one of the largest financial threats facing consumers, title companies, and our real estate system. My wife and I own H.B. Wilkinson Title Company in Galena, Illinois. We bought the company from my dad 20 years ago. We have 28 employees, with offices in seven counties. We close about 70 real estate transactions a month. Though we are a small business, by title industry standards, we are a big company.

One of my favorite opportunities as president of ALTA was traveling the country to hear what was happening in local markets. The largest concerns I heard from title agents were on data security and the growing threat of criminals trying to steal our customers' money. Even my small company in Galena sees a couple of phishing attempts every week. Those attempts are often sent to multiple email addresses.

Earlier this year, the FBI reported a 480 percent increase in criminals attempting to steal consumers' funds, and it is easy to see why. The average successful bank robber's haul is \$3,816. The average successful wire fraud loss is \$129,427. This is a much better return for a much less expensive and dangerous crime to commit. Overall, these scams have cost Americans \$5.3 billion.

Home buyers are the most common targets. Criminals gain access to the buyer's, seller's, or real estate professional's email ac-

count. They monitor traffic looking for a deal. Their goal is to convince the buyer to send their earnest money or downpayment to the criminal. Bloomberg reports that criminals can obtain verified email accounts, passwords, and security questions on the dark web for as little as \$10.

In Texas, I heard about a woman who saved nearly \$25,000 for the downpayment on her first house. Prior to the lender finalizing the closing disclosure, the woman's email was hacked. Using information from her email, the criminal impersonated the title agency, used the closer's name, and instructed her to send the \$25,000 using fraudulent wire instructions. Believing it was the title agency, she followed the instructions and wired the funds to the criminal's account. The home purchase fell through. The money was gone. The woman lost her life savings. This is a heartbreaking story, and it happens often. Title companies in each of your communities have stories just like these.

Consumer losses due to a data breach pale in comparison to the loss of consumers' downpayment or earnest money deposit. I wish there was a silver bullet to protect our customers, but there is not. As an industry, we have improved our digital hygiene and have taken an array of steps to combat this fraud. This includes using secured email communications, verifying instructions with buyers using known phone numbers, and asking banks to match both the recipient's account number and payee information when we send wires. We issue warnings to our customers on websites and at the bottom of every email.

What is so frustrating is there is no amount of money we can spend to protect our customers from being targeted by these criminals. Two years ago, we were the target, as title settlement agents. Now they are targeting our customers even before we get involved in the transaction, because we are at the end of the process.

We believe we should focus on two key areas to stop these crimes. First, we need to increase awareness of these crimes for buyers, sellers, and the public. We need to get anyone involved in the real estate deal, real estate agents, banks, policymakers, consumer groups, title insurers, settlement agents and real estate attorneys, to help educate our customers about how to protect themselves. Think about movers. Think about surveyors, home inspectors. They are all part of the process.

Second, financial institutions should match not only the account number, but also the payee's name. This simple authentication step can be the single biggest deterrent. We also need to better use both suspicious activity reports and IC3 data to detect trends. Even if more information does not lead to prosecutions of these criminals, it can help banks decide to place holds on the account to prevent the criminal from withdrawing funds.

ALTA is eager to serve as a resource to the subcommittee, and I am happy to answer any questions. Thank you.

[The prepared statement of Mr. Mennenoh can be found on page 50 of the appendix.]

Chairman LUETKEMEYER. Thank you, Mr. Mennenoh.

Mr. Mierzewski, you are recognized for 5 minutes.

STATEMENT OF EDMUND MIERZWINSKI

Mr. MIERZWINSKI. Thank you, Chairman Luetkemeyer, members of the committee.

Last week, you held a minority day hearing on Equifax. I could talk about Equifax for my entire 5 minutes, but I think the State enforcement officials and the consumer advocates who spoke last week, I would simply like to associate my remarks with theirs last week on Equifax specifically. But I do want to continue to talk a little bit about how Equifax fits into the larger big data universe.

First of all, to be clear, Equifax had one of the worst breaches ever. They lost our consumer DNA through a pretty amazing failure to protect it, and then they did a really bad job of notifying us and telling us what was going to happen after that. But what people don't understand, a lot of people may not know, Equifax is in the highly regulated business, credit reporting, part of the time, but all of the time Equifax is a data broker. There are thousands of underregulated and unregulated data brokers out there.

In my testimony, I represent the views of the Federal Trade Commission which has said they need more authority over data brokers. I encourage the committee to read their reports.

Going forward, people should understand that consumers have no control over their information, particularly with the credit bureaus. As was said often in many of the other hearings, we are not their customers; we are their products. Mr. Cordray refers to credit reporting as a dead-end market. You can change your bank if you don't like it. You cannot change your credit bureau. You cannot vote with your feet.

With the lack of control, it is very difficult for consumers to do anything about misuse of their information. We have very little authority to vote, to determine that companies can't use our information, very limited under Gramm-Leach-Bliley. In most cases, companies simply collect information about us and sell it.

We worked on the credit freeze as a way to return some control, starting about 20 years ago. The first credit freeze law passed in California about 15 years ago. It was revolutionary at the time, but what would make it more revolutionary is if the committee were to adopt—and I believe it has become a bipartisan issue—expand the availability of the free credit freeze. It is the only way you can at least exert some control over your consumer DNA. In addition, the committee should look at Ranking Member Waters' comprehensive bill to reform the credit bureaus themselves.

Third, I think the committee should look very closely at the flaw in Gramm-Leach-Bliley where the Federal Trade Commission has authority over data security that was not transferred to the Consumer Bureau. Section 1093 should be looked at. I think the Consumer Bureau, because it has the ability to conduct examinations of credit bureaus, because it has the ability to impose penalties for the first violation of the law, not only after a company has violated a consent decree in the FTC's case, and because it has rulemaking authority that the FTC does not have. If you want to rein in the credit bureaus, you have to give the Consumer Bureau more power over them.

The final point that I want to make in my testimony, and I make it extensively in my written testimony, is that the States are pri-

vacy innovators. The States are privacy first responders. The credit freeze, the data breach notification laws, all were passed by the States when Congress looked on and didn't do anything.

We strongly support protecting the right of the States, as the two attorneys general offices testified last week. Going forward, we cannot preempt stronger State laws with some narrow Federal breach law that takes away States' rights not only to do breach notification, but States' rights to conduct other privacy examinations, and States' rights to strengthen the data security of their citizenry.

I go into great detail on all of these matters in my testimony. I look forward to your questions. Thank you.

[The prepared statement of Mr. Mierzwinski can be found on page 61 of the appendix.]

Chairman LUETKEMEYER. Thank you, Mr. Mierzwinski.

Ms. Schwartz, you are recognized for 5 minutes.

STATEMENT OF DEBRA SCHWARTZ

Ms. SCHWARTZ. Chairman Luetkemeyer, Ranking Member Clay, and members of the—

Chairman LUETKEMEYER. Please turn on your microphone.

Ms. SCHWARTZ. It should be on.

Chairman LUETKEMEYER. Bring it closer to you then. There you go.

Ms. SCHWARTZ. OK, thank you.

Chairman Luetkemeyer, Ranking Member Clay, and members of the subcommittee, thank you for the invitation to appear before you this afternoon. My name is Debra Schwartz, and I am testifying today on behalf of NAFCU. I currently serve as president and CEO of Mission Federal Credit Union, Mission Fed, headquartered in San Diego, California, and also serve on NAFCU's board of directors as treasurer.

Data security needs to be everyone's responsibility. More can and must be done to protect consumers on this important issue. NAFCU has long supported comprehensive data security measures to protect consumers' sensitive data. Credit unions and other depository institutions already protect data, consistent with the provisions of 1999's Gramm-Leach-Bliley Act, GLBA.

Unfortunately, there is no similar regulatory structure for other entities that may handle sensitive personal and financial data. Although credit bureaus are considered financial institutions under GLBA, they do not have the same regulatory oversight as credit unions and other depository institutions.

GLBA and its implementing regulations have successfully limited data breaches among depository institutions. This standard, outlined in my written testimony, has a proven track record of success and should be recognized in any future requirements. Gramm-Leach-Bliley requires financial institutions to address the risks presented by the complexity and scope of their business. This allows flexibility and ensures the regulatory framework is workable for the largest and smallest financial institutions. GLBA is an example of how scalability is possible for varying size businesses.

A data security breach can have a big impact on consumers, from waiting for new cards to be issued to updating all accounts connected with a compromised card. Breaches can also result in fraud

losses, damaged credit ratings, and even identity theft. As the Equifax breach has demonstrated, data security breaches are not just a retailer problem, but occur across many industries. This highlights the need for a comprehensive national data security standard to protect data, akin to what is already in place for depository institutions under GLBA.

A recent survey of NAFCU members found that respondents were alerted to potential merchant breaches an average of 189 times in 2016. Over 40 percent of the respondents said that they saw an increase in these alerts from 2015. At Mission Fed, we have received over 1,400 separate alerts of merchant data breaches since 2013.

When credit unions are alerted to breaches, they take action to respond and protect their members. These actions have costs, such as card reissuance, fraud losses, and account monitoring. Ultimately, this takes away from providing other services to members. Unfortunately, credit unions rarely see any reimbursement for these costs. Even when there are recoupment opportunities, such as settlements, it is usually only pennies on the dollar, in terms of the real cost and losses incurred.

Recognizing that finding a legislative solution is a complex issue, NAFCU has established a set of guiding principles we would like to see in data security legislation, including: reimbursement of all costs by the breached entity; national standards for safekeeping of information; breach notifications to financial institutions; disclosure of breached entity to consumers; and enforcement of data retention prohibitions. I outline all of our principles in detail in my written testimony.

The time has come for Congress to enact a national standard on data protection for consumers' personal financial information. Additionally, credit bureaus, such as Equifax, should be subjected to examinations for compliance to data security standards, just as depository institutions already are. Consumers whose personal and financial data has been compromised have a right to be notified in a timely manner.

NAFCU believes that the best legislative solution so far on this issue of data security is the bipartisan legislation that was introduced in the 114th Congress, H.R. 2205, the Data Security Act of 2015, which would have set a national data security standard that recognized those who already have one under the GLBA. We were pleased to see this bill get bipartisan support in this committee in the last Congress.

Finally, as the committee is aware, data security is in the jurisdiction of several congressional committees. We appreciate the Financial Services Committee taking the lead to work with leaders in other committees to craft a bipartisan package that can enact a robust national data security standard into law.

In conclusion, data security is a top challenge facing the credit union industry today. Protecting the payment system is the responsibility of all parties involved. It is time to level the playing field, establish a national data security standard for all who handle financial and sensitive personal data. This includes consumers and impacted parties receiving timely notification of data breaches.

The standards for depository institutions under GLBA should be the model. NAFCU stands ready to work with you. Thank you for the opportunity to appear before you today. I welcome any questions you may have.

[The prepared statement of Ms. Schwartz can be found on page 78 of the appendix.]

Chairman LUETKEMEYER. Thank you, Ms. Schwartz. I appreciate your testimony and all of the witnesses today.

We will now begin the question-and-answer period of our hearing, and the chair recognizes himself for 5 minutes.

Mr. Bentsen, you in your testimony talked about harmonization of State and Federal data security regulations. You even mentioned global standards. Where in this do you think this committee has a role to be able to help the situation the way it is right now?

Mr. BENTSEN. Thank you for the question, Mr. Chairman. It is a problem where the industry and the government are all trying to get to the same place. There is very little disagreement on that, and we believe it is very much a two-way street.

We have a multifaceted regulatory structure for financial institutions, including both a Federal and State regulatory structure, and self-regulatory organizations, and we have many global institutions from the U.S. that operate in multiple jurisdictions. We need to find a way where regulators can come together, in terms of the type of guidance they are doing, the examinations, the supervision process that they want to do, to work around the same framework. Even in the U.S., U.S. regulators are not all using the NIST framework, which we think is the best framework for developing cyber resiliency.

I think this committee can play a role with your oversight function of the agencies to start, and the SROs, where you have some indirect jurisdiction, to try and bring them together. To be fair, we have spent time with all of our regulators, brought them all together and said: We understand your individual mandates, but cyber and cyber protection is really a top-of-the-house-down program within all institutions.

There has to be a better way to do this, so we don't have a situation where members are spending almost as much time on regulatory compliance as they are on cyber defense.

Chairman LUETKEMEYER. OK. With regards to the NIST standards, do you believe that they are adequate at this time and, if not, what concerns do you have, and in particular, with regards to notification? I am very concerned about notification. It doesn't seem like we have either some standards in place or they are not being adhered to. Can you elaborate a little bit on that?

Mr. BENTSEN. We think the NIST framework is the appropriate framework. It has been updated recently by NIST. We think it provides sufficient flexibility to the industry. We have mapped it out for our industry, and the capital markets and asset management business and other sectors are using it as well.

In terms of notification, this is an important issue. I think everyone agrees that there does need to be timely notification. But I think we also have to be careful in setting deadlines that can be artificial, and we have to determine what the materiality is. We have to determine—in many cases, you can have a cyber event

going on and you are in the process of trying to figure out how deep it is, what the impact of it is, if you have to do a forensic audit, if you have to call in the FBI, if it involves—whoever the perpetrator is, and to also be up against a deadline of having to notify before you know what is really going on adds additional risk factors.

It is an important issue. As you know, Chairman Clayton of the SEC has raised this issue under the jurisdiction of this committee. I think it is something that, you all and the agencies are going to be spending a lot of time on.

Chairman LUETKEMEYER. Thank you.

Ms. Schwartz, you were talking about the GLBA quite a bit. Do you believe that it is still adequate, or do you see some things that need to be changed in it or amended or added to, or what do you think?

Ms. SCHWARTZ. GLBA has been around since 1999, and it has been dynamic, scalable, and flexible. The nice thing about it is it works for institutions, whether you are a \$10 million credit union or a multibillion dollar credit union. I think it provides an excellent model to be considered, because of those factors.

Chairman LUETKEMEYER. OK. With regards to notification, there is not a whole lot in Gramm-Leach-Bliley with regards to notification. Can you expound on what your position would be with regards to where we need to go with this? Do we need to put some guidelines in place or leave it alone or—Mr. Bentsen just indicated there are a lot of problems with how you go about that, but is there a way we can get through this and find a middle ground here?

Ms. SCHWARTZ. Notification is key. We found out about the Equifax breach probably the same time you did, when we read about it in the Wall Street Journal. We subscribe through Mastercard, who is our credit card partner, and receive ADC notifications from them. We have received 1,400 separate breach notifications since 2013. The faster we are notified, the faster we can work to protect our members, by putting warnings on their account, by reissuing cards. It is absolutely critical that we get notification as soon as possible.

Chairman LUETKEMEYER. I have just a few seconds left.

Mr. Bentsen, you mentioned the Consolidated Audit Trail and the compounding of all information in there. Do you think that is really a good idea?

Mr. BENTSEN. Well—

Chairman LUETKEMEYER. Very quickly. My time is up.

Mr. BENTSEN. Yes, the concept behind Consolidated Audit Trail is we think an appropriate concept. But we don't know that the question has been answered that you have to have all this personal information as part of the Consolidated Audit Trail in one place. We have no assurance from the builders and the contractor that they can protect it.

Chairman LUETKEMEYER. OK, thank you. My time has expired.

With that, we go to the gentleman from Missouri, another gentleman from Missouri, the ranking member. Mr. Clay, you are recognized for 5 minutes.

Mr. CLAY. Thank you, Mr. Chairman.

This question is for the entire panel, so we would start with Mr. Bentsen and go down the line. Good to see you again, Mr. Bentsen.

Equifax learned of the data breach on July 29th, 2 days after it filed its quarterly report with the SEC. However, it was not until 6 weeks later, on September 7, that Equifax notified the public of the breach through a statement filed with the SEC.

Now, in your view, what duties do public financial services companies owe consumers to provide timely notice of significant cybersecurity incidents? Do you believe that disclosure 6 weeks after a material event is timely? Could you elaborate whether this extended period with the Equifax incident, from when the company learned of it to when the public was made aware of it, may have violated some State breach notification laws, particularly given that some States require immediate notification and most States require notification within the most expedient time possible without reasonable delay?

I will start with Mr. Bentsen and would like for each panelist to try to answer some of those questions.

Mr. BENTSEN. Thank you, Mr. Clay, and good to see you again as well.

First of all, Equifax is not a member of ours. We don't represent the credit bureaus. Most of what I know about the Equifax issue is what I have read in the press. I can't really comment on what they did, whether it is appropriate or not, and I am sure the appropriate regulators are looking at the issue as it is.

Again, I think there is a question of materiality. There is a question of your risk factors, when there has been a breach and if the person who is breaching is still there and who it is and how you are dealing with it. There is no question that there should be an effort to notify the affected parties, your clients in this case, as soon as it is practical that you can do so, weighing all those other factors.

As it relates to Equifax they are not a member. I am not familiar with the facts of that case.

Mr. CLAY. Sure. But you are saying they did have a duty to inform the public.

Mr. BENTSEN. I think if it is a material issue, there are a number of requirements, both in terms of public company requirements and State—and I can't speak to all the States; Ed probably can—of what they have to comply with.

Mr. CLAY. Mr. Mennenoh.

Mr. MENNENOH. Thank you, sir.

Yes, I certainly would agree that consumers need to be notified promptly. Certainly from our perspective, when we have circumstances where consumer funds have been taken, we take immediate action to try to recover those funds. But with wire transfers, oftentimes, it is a case where if you don't address it within 24 hours, it is pretty difficult to get those funds back.

Mr. CLAY. 6 weeks was, in your opinion, quite a bit of time expired?

Mr. MENNENOH. For our purposes, the money is gone.

Chairman LUTKEMEYER. Mr. Mierzewski.

Mr. MIERZEWSKI. Mr. Clay, I totally agree. You made a lot of the points in your opening remark here. Equifax probably violated the

strongest State laws on immediate notification. It probably violated a number of State laws on attorney general notification. Massachusetts has already sued Equifax. Other State attorneys general have a multiState investigation going on right now. I think you will see additional litigation against the company. You will see private lawsuits as well. But they failed. They epically failed, and a lot more needs to be done.

Mr. CLAY. Thank you.

Ms. Schwartz.

Ms. SCHWARTZ. Six weeks is clearly too long. I think, in addition to notifying consumers, notifying financial institutions is also critical. We are in a position where we can really help to mitigate fraud. We can put warnings on accounts; we can reissue cards. We can't do that if we are not told. A lot of fraud can happen in 6 weeks.

Mr. CLAY. Mr. Mierzwinski, in the event of a breach, what information should be provided to consumers to ensure they are fully informed of the rights and remedies available to them as well as the steps that they consider taking to protect against fraud, identity theft, and other crimes?

Mr. MIERZWINSKI. I think consumers need to hear everything about their rights under Federal law and what the company is going to do, and they don't need to hear about all the changing kinds of results that Equifax provided them. You need to know what your rights are. You need to learn how to put a fraud alert. You need to learn how to put a credit freeze on. You need to learn all of these things. You need to understand that your Social Security number is the key to identity theft. They lost that. It is much worse than any merchant breach.

Mr. CLAY. Thank you.

My time is up.

Chairman LUETKEMEYER. The gentleman's time has expired.

With that, we go to the gentleman from Texas. Mr. Williams is recognized for 5 minutes.

Mr. WILLIAMS. Thank you, Mr. Chairman.

Thank all of you for being here today, and I appreciate your testimony this afternoon on the important subject of data security and how we can and must do better to protect private information.

As a small business owner for 45 years, I recognize the importance of protecting the information of my customers, and I know firsthand the impact that cyber attacks can have on Main Street America.

I am concerned by the increasing trend of breaches that has occurred over the past few years, and I hope to learn from all of you today how we can ensure that American consumers can rest easy, knowing that their personal information is in good hands.

Mr. Bentsen, one of the things that I do worry about, not just when it comes to the industry but in general, is an issue with excessive regulations. When President Trump was elected, he pledged to fight against expanding the regulatory regime. I agree with his goals on that regard. One of the fears I have, which you also mentioned in your testimony, is that Congress creates regulations which result, I quote, "in requirements which are sometimes overlapping, duplicative, and conflicting."

How can Congress create effective rules while avoiding the problem of overburdensome regulations?

Mr. BENTSEN. I think in the case of cyber protection, including protection of sensitive data like PII, I think Congress plays a very important oversight role with the agencies that you set the authorization for, you fund, you set the laws that they execute on.

In the case of the financial services sector, where you can have 5, and up to 13 different regulators, Congress can definitely play a role in trying to get better coordination among those regulators in how they are going to implement cyber rules, cyber defense rules, guidance, or whatever it may be, as well as on their examination process.

We have members who, again, they have up to 13 different regulators before you get to the States. We have members who are going through multiple examinations because they have a bank, a broker-dealer, a futures commodities merchant. In many cases, they will have the SEC, the CFTC, the OCC, the Fed coming through, but that is before whoever their State regulator may be or whoever their SRO may be.

If we can get some harmonization there, where we are all trying to do the same thing, and with Congress' oversight function working with those agencies, that could be very helpful.

Mr. WILLIAMS. Thank you.

Mr. Mennenoh, this question is for you. I mentioned earlier my background as a small business owner, and I am extremely concerned with protecting the nonpublic personal information of my customers. I am a car dealer.

In your testimony, you discuss how the American Land Title Association, which represents many small businesses, has developed a set of voluntary standards for its members to use as part of their compliance programs. Can you expand on these standards, and to what extent do your members cooperate with law enforcement following a breach, and what steps would you recognize to take immediately following a breach?

Mr. MENNENOH. Thank you. Yes, the standards that we put out, the voluntary ALTA best practices, do address very specifically how to protect data, how we should be addressing that in quite a bit of detail. But the other side of it too is that because we handle a lot of money for real estate transactions, we also have to protect the money. We have very high standards in terms of how we protect the money as the transactions are taking place.

It is a process that we feel has raised the bar, if you will. I believe many of our members are doing a very, very good job of addressing this, but, as I mentioned in my testimony, the biggest issue for us is the money at this point. The small companies often-times use third-party data centers, that sort of thing, that have high security standards for the data security, but we have to make sure that we are protecting the money as well. That is a big issue for us, and we address this very, very aggressively.

Mr. WILLIAMS. Thank you.

Ms. Schwartz, one of the biggest issues in the wake of the Equifax breach was their notification process to consumers. In your testimony, you too acknowledge that Equifax failed in the area of consumer notification. Additionally, you discuss the need for timely

notification of members after a breach has taken place. In your words, you say that this is important to manage an institution's reputation risk.

What kinds of notification standards should Congress consider requiring, if any, and would such standards hamper the efforts of law enforcement following a breach?

Ms. SCHWARTZ. I think the most important thing is trying to avoid the breaches in the first place. But absent that, timely notification as soon as reasonably applicable. It is very difficult to put a certain timeframe on it, because I think there are issues, such as law enforcement actions, that could possibly delay it. But as soon as possible, financial institutions can do a lot to help mitigate any losses that could happen. We can reissue cards. We can also notify our members that their accounts have been compromised. We have a pretty good track record of them opening up the emails that they get from us.

The notification standards as they are right now can be somewhat nebulous, particularly in California; I believe you can just put something in the newspaper. It puts a lot of pressure on the consumer to look up to see if it has been compromised. There is a lot of room there for improvement.

Mr. WILLIAMS. Thank you for your testimony.

I yield back.

Chairman LUETKEMEYER. The gentleman's time has expired.

With that, we go to the distinguished gentleman from Georgia. Mr. Scott is recognized for 5 minutes.

Mr. SCOTT. Thank you very much. Mr. Chairman, this issue is very important to all of the American people and all of us Members here in Congress, but it is expressly important to me because I am the representative from the great State of Georgia, a State I love. This extraordinarily careless breach that was allowed at Equifax is certainly very troublesome to me. I am very concerned about that. I have a commitment to help Equifax because I want to make sure that we can bring them out of this standing tall, standing big, and be able to renew the confidence of the American people. However, that is not going to happen for any of them, but certainly for Equifax: 145 million people, and their Social Securities are out there in the wind, their birth dates, all this vital information.

While I want to do that, we on this committee and Members of Congress, can't do it without them. I don't know if you all know this, but they refused—can you imagine that?—to come before this Congress and speak. We cannot solve this problem, you and I. I know many of you.

Mr. Bentsen, I know your great reputation.

Ms. Schwartz.

All of you. But neither you nor I can solve this problem if the CEOs, the people that run Equifax, that run TransUnion and these other companies are not willing to come and sit where you are so that we can find that. We have to get the message to these credit agencies that they have to get here in Congress, partner with all of us. This is a huge issue. I just hope that you all will convey that message to them.

Now, with the time remaining, I just want to—I look at this as the American people look at it and want to get your responses to

this. If Americans can't trust their credit and data, that it is going to be protected, let me ask you this, Mr. Bentsen, Ms. Schwartz, any of you: Why would they want to risk shopping online for their Christmas gifts? Can you see the damage that this would do to our economy through that? Or if Americans don't think that their local banks can keep their personal account numbers protected, why would they want to risk it by opening up a checking account?

In other words, the whole foundation of our fantastic and yet complex financial system is registered in credit. If these credit agencies, 145 million Americans, Mr. Bentsen, I ask you and Ms. Schwartz, how many of these 145 million Americans do you believe even have been informed that their data is out floating and gone with the wind?

Mr. BENTSEN. Mr. Scott, I don't know the answer to that question, but certainly there has been a lot written about it, and I have been on the website myself.

What I will say, I think you are absolutely correct that there are two things that are very important. The confidence in the system is incredibly important. In the industry at large—we don't represent the credit bureaus, so I won't speak for them. The industry at large has a responsibility to work to maintain that confidence, and this industry does that day in and day out. No. 1, it is through defense; and No. 2, it is through recovery. We are taking efforts in both those areas, including understanding what happens if you have a major attack wiping out books and records. Can someone at the end of the day go back and say: What was my balance of my retail brokerage account yesterday? What was my balance in my checking account yesterday?

These are the things we should be working on, which we are.

Mr. SCOTT. Ms. Schwartz, let me ask you, because I have been concerned about Gramm-Leach-Bliley standards and the applicability of them to large as well as the smaller, the rural companies. I think you alluded to this in your testimony, and I would like for you to clear that up.

Do you have confidence in that one size will fit all? Particularly when you look at our economic system, it is so diverse; it is so varied. To have the same standards for a big mega bank operating around the world, for a mom-and-pop store in my district in Stockbridge, Georgia? Are you saying that we don't have to worry about that, that it is applicable?

Ms. SCHWARTZ. No, I think your point is very well taken. One size fits all is not the answer. But I will say that the beauty of Gramm-Leach-Bliley is it is scalable, and it is flexible. It has been around for more than 17 years and is still helpful and provides a framework. I think a level playing field is very important. Some minimum standards that anyone along the payment system rails should follow I think is very important.

Mr. SCOTT. Thank you.

Thank you for the little extra time there, Mr. Chairman. I appreciate it.

Chairman LUETKEMEYER. Thank you, Mr. Scott.

The gentleman's time has expired.

With that, we go to the gentleman from Michigan. Mr. Trott is recognized for 5 minutes.

Mr. TROTT. Thank you, Mr. Chairman.

I also want to thank the panel for their time this afternoon.

Mr. Bentsen, I want to start with you. You talked in your opening comments about the need for partnership between industry and government to address this problem. I am just curious what is the most significant barrier in your mind to the creation of that partnership, and what does that partnership look like? Is it just less, more reasonable compliance, burdens, or what does the partnership look like, and how do we accomplish it?

Mr. BENTSEN. Congressman, thank you for that question. I think our partnership with the government on the broad question of cyber resiliency is quite good. I credit the Treasury Department, Homeland Security, and the various agencies for that. This is something where everybody is trying to row in the same direction. Frankly, through a lot of industry exercises and a lot of tabletop exercises with the government, and we have learned a lot. They have learned a lot, I think. We have learned a lot from them as well, and we want to keep doing that. That has led to new initiatives on both sides, I believe.

Where I think things can break down is agencies operating under their own individual mandate, which is established by law and all of that. That is understandable, but it seems to us that we can do a better job of coordinating among those various agencies so there is more interchangeability between how firms are complying with requirements. That is really the point.

Mr. TROTT. Maybe 2 or 3 instead of 13 would be a good start?

Mr. BENTSEN. Or some substitution, yes.

Mr. TROTT. Thanks so much.

Mr. Mennenoh, nice to see you again. We met up in Traverse City at the Michigan Land Title Association. You were the keynote speaker up there this summer.

Mr. MENNENOH. Yes, we did.

Mr. TROTT. I hope you enjoyed your time in northern Michigan.

Mr. MENNENOH. Absolutely.

Mr. TROTT. You discussed wire fraud and what a huge problem it is for the industry. It is a significant problem because, unlike some of these issues, really there is no good solution. Once it happens, the money is gone. Usually it is a lot of money, as you said.

You discussed education, and it sounds like a good idea, but I wanted to get your thoughts on—one thought I had was maybe we put some kind of disclaimer or warning in the purchase agreement, or maybe the realtor's listing agreement has some kind of—or there is some form. But, that is probably not a great solution, and I want to get your thoughts on it, because you have a buyer who is excited to get their home. Maybe it is their first home. They don't even understand what a title agency does in the overall transaction, perhaps. Is the education going to make a difference, or is it really the financial institutions that have to be the solution in terms of the wire fraud?

Mr. MENNENOH. Honestly, I think there is maybe a combination of the two. Certainly the financial institutions, if we can match the account name, the account owner to the account number and the routing number on a wire transfer, that would actually be a good deterrent.

But I also think the education component is very important as well, in that all of the professions involved in real estate can work together, send the same message. It has to be a message that is being conveyed routinely, because, as you say, people buy a house and they may not buy another house for years. But providing that level of education from all of the professions that are involved in this process would be very, very helpful.

As I mentioned before, we are at the end of the process. The parties that have first contact with the consumer can help with that process as well. For example, in January, I, along with the Board of Governors at ALTA, met with Director Cordray, and we were asking for a consumer alert to be issued. The Director's initial response was, how often does that really happen? We were telling him stories about things that have, in fact, happened.

We followed up again in April. Then it wasn't until June that we actually had the CFPB issue a consumer alert. That is all we wanted to have them do. It is a difficult process.

Mr. TROTT. That is for sure. Thank you.

Ms. Schwartz, so my friend from Georgia was quite articulate in how he described the ramifications to commerce, e-commerce in this country, given the Equifax breach. I want to ask a question with respect to Mission Federal. Can you say with 100 percent confidence that you can build a firewall that will protect your members' data?

Ms. SCHWARTZ. I don't think anybody can say with 100 percent confidence, but I can tell you we have had 245,752 attacks on our system through September 30th, none of which were successful.

Mr. TROTT. That is extraordinary. But your answer, I was hoping you would say that you couldn't say with 100 percent confidence that you could protect the data, because I think that is an accurate answer.

My concern is, when we talk about notification and we are beating up Equifax for how poorly they handled that whole process, to some extent, we were really in damage control at that point. When we talk about a solution—and I am out of time here—I wonder if really we need to focus on a solution that changes the identification process that goes well beyond a Social Security number and date of birth and really makes it much more cumbersome for these cybercrimes to happen.

But I will yield back. Thank you for the additional time, Chairman.

Chairman LUETKEMEYER. The gentleman's time has expired.

With that, we go to the gentlelady from New York, Mrs. Maloney. She is recognized for 5 minutes.

Mrs. MALONEY. Thank you. I thank the chairman and ranking member for calling this important hearing and take this opportunity to welcome my former colleague and very good friend Ken Bentsen. We miss you. I hope you will run for Congress again. But, anyway, it is good to see you again.

My question to Mr. Bentsen and actually everybody on the panel, as you know, last Congress, this committee considered a data security bill that would have created a national standard for data security and for breach notification procedures. I supported that bill because it would have subjected many more companies to the strong

data security requirements that financial institutions already have, subject to the safeguards rule.

But we cannot ignore the fact that Equifax was already subject to the safeguards rule, which is what the legislation would have done, yet it still suffered a massive data breach that affected a startling 145 million Americans. Not just today but for the rest of their lives, they are in threat with their security, their identification stolen, their Social Security number.

My question to all of you is, in light of the Equifax breach, do you believe the safeguards rule needs to be updated at all to include things like encryption requirements and the two examples of startling mismanagement by Equifax.

I know Ms. Schwartz was saying that you should have training so that you would be looking for these breaches. But in an unprecedented action, Equifax was notified by the Homeland Security Department that you will be breached: You will be breached in this way; take steps to protect your customers.

Now, the other two companies took steps to protect their customers. Equifax did not. No matter how many training sessions you had, if someone tells you you are going to be breached this way and you don't correct it, training is not going to help you.

The other two companies, it is my understanding—because I wrote them and they wrote me back and said they had these other safeguards—they had a system that once you told their system that there could be a breach in a certain way, the whole system closed down until you corrected it. Should Equifax be required to have the same updated system?

Also, Equifax had a system that was different from the best practices that were put out by the safeguards rule. The best practices said that every firm should have an IT manager who is in charge of this, who is responsible. The other two firms had an IT manager whose sole job was to protect their customers, protect the system, make sure it is safe, but Equifax did not. They had everybody reporting to a, quote, "general manager," who had conflicting responsibilities, such as managing the whole company, the general counsel, such as profits, such as new technologies or whatever else he was looking at. He wasn't focused on IT.

Should that best practices idea that has been put out there be implemented in law so that people are following it? We have to take steps to make sure that this happens. Or do you just need to enforce the safeguards rule more?

I would like to really go first to my colleague Mr. Bentsen and down the line. I know he has sponsored some data security forums that I have been privileged to attend. I would just like to hear your comments on what we need to do to protect this information. I am astounded that they were notified by the Homeland Security Department and they still couldn't figure out how to correct a breach that they were told they were going to get.

Mr. BENTSEN. How you describe the situation with Equifax would not be consistent with how the financial services industry approaches the issue of cyber defense, preparedness, and resiliency. And the industry is doing a lot on its own, through its own self-directed principles, in adhering to the NIST framework.

Furthermore, though, our regulators will regularly look and see how we are complying with our cyber defenses and resiliency. Our concern is doing it 13 times the same way, but that is more of a process question.

That would not be acceptable within our industry.

Mrs. MALONEY. Any other comments?

Ms. SCHWARTZ. I think examination is an important part of that. In the credit union industry, we receive regular examinations. There is not a regulatory body that routinely goes into any of the credit bureaus and ensures that they are following those best practices.

We just completed a regulatory exam last Friday where they asked us to have a backup firewall to our backup site. We have a firewall, a backup firewall, a redundant site, and a backup firewall for that. I don't believe that the credit bureaus are subject to that same degree of scrutiny and examination.

Chairman LUETKEMEYER. The gentlelady's time—

Mr. MIERZWINSKI. Could I make a brief comment?

Chairman LUETKEMEYER. Very brief.

Mr. MIERZWINSKI. Very briefly, Congresswoman, the Equifax mess is a mess, but the solution is examination authority. I think it should go to the Consumer Bureau. They have all the rest of the authority over Equifax, but everything they did was wrong.

Chairman LUETKEMEYER. OK. The gentlelady's time has expired. We go to the gentleman from Colorado, Mr. Tipton, recognized for 5 minutes.

Mr. TIPTON. Thank you, Mr. Chairman, and thank the panel for taking the time to be able to be here. I would like to start with Mr. Bentsen, in your testimony you had noted that approximately 40 percent of cybersecurity activities were focused on compliance rather than security.

How is that impacting the ability to actually address what I think people are concerned about, and that is actually having real security?

Mr. BENTSEN. That is what our member firms report to us, in terms of having to deal with various compliance requirements, exercises, and all. Again, our point is we understand the need for this, but it is having to do it over and over and over again when—and having to deploy those resources when they could be deployed to frontline defense and resiliency and recovery planning.

Second, I would point out, which is not in my testimony, but industry statistics have found that there is actually a shortage of cyberdefense personnel in the United States. This is something where I think we ought to be careful how we are deploying our resources. That we are not overtaxing when we don't really need to. We can accomplish the same thing for different regulators because of the way the industry approaches the question.

Mr. TIPTON. Well and you have spoken a lot to the harmonization that needs to happen. Would this actually help in terms of harmonizing some of the policies that are going through the different agencies so you aren't filing duplicate reports to the 13 different agencies to be able to address that?

Mr. BENTSEN. We think so. We are talking with our regulators about that. Again, we are all trying to do the same things. We can

use the same nomenclature. We can try and adhere to the same framework, which we think it ought to be the NIST framework. If you were able to have a good exam with SEC, you ought to have a good exam with FINRA, likewise with the OCC, or whoever it may be.

Mr. TIPTON. Yes. Ms. Schwartz, is that pretty much your experience with the credit unions as well? Are you seeing dollars for compliance as opposed to security?

Ms. SCHWARTZ. It is absolutely true. But as a credit union, we are in the trust business a little bit as well, well, a lot as well, and our reputation is very, very important. Even absent the regulations, absent the compliance requirements, most of the things we would be doing anyway, because we would absolutely lose our membership if they can't be 100 percent confident that we are protecting their secure information, their private information.

Mr. TIPTON. Right. A lot of the concern really is about having that real confidence within the system. I think, probably everybody can agree there will be a tax, there will be breaches that are going to take place.

Mr. Bentsen, through SIFMA, you have developed a program, I think through your industry, the Quantum Dawn, to be able to identify maybe some responses, to be able to rebuild those databases.

What has been something that you have learned from that?

Mr. BENTSEN. Congressman, the Quantum Dawn is a industry-wide exercise that we do biannually, and do simulate major attacks on market infrastructure, different sectors of the industry, with our government regulators looking over our shoulder. From those we learn a number of things, including better ways of information sharing, who you should call in the Government, depending on what type of account. Testing our playbooks and our recovery playbooks, for instance, of whether markets should open or close if there is a major attack on an infrastructure situation.

The industry finds this very valuable. Our regulators, I think, find it very valuable. We have also done tabletop exercises with our regulators and going through different scenario planning. In those we have actually also come up with things that neither us nor the Government necessarily had thought about, and that has led to new initiatives that we think improve our resiliency.

Mr. TIPTON. Speaking to that, would you maybe speak a little bit to the Sheltered Harbor?

Mr. BENTSEN. The Sheltered Harbor is an initiative that came out of what is known as the Hamilton Exercises, which is a Treasury-led effort with the industry and the Government. Sheltered Harbor is an industry-led effort that SIFMA as well as the ABA, the FSR, the Clearinghouse, and a number of other industry participants and vendors participate in. It is now housed under the FS-ISAC.

The idea here is if there is a major attack on a banker, broker, dealer, and all of their data is wiped out, and they are not able to stand back up. Are you able to recreate end of day balances from the day prior—and bring that up through a vendor or another institution. It is done through establishing a protocol that firms would adhere to. We are currently at about 70 percent of the bank

retail deposits participating in the process, and about 50 percent—or 60 percent of broker dealer retail accounts.

The idea is, again, to be able to go back through encrypted offline protocol that then could be reestablished. Again, it goes back to the question of confidence in the system in trying to solve that. That came out of our exercises. We didn't have a mechanism in place so now we are trying to create it.

Mr. TIPTON. Great. Well thank you. My time has expired, Mr. Chairman.

Chairman LUETKEMEYER. The gentleman's time has expired. With that, we go to the gentleman from Tennessee, Mr. Kustoff, you are recognized for 5 minutes.

Mr. KUSTOFF. Thank you, Mr. Chairman. Thank you to the witnesses for being here this afternoon. Mr. Mennenoh, if we could, I know in your testimony you discussed the rapid increase in criminal attempts, almost—I think you said almost 500 percent—480 percent.

Mr. MENNENOH. Yes.

Mr. KUSTOFF. To steal customers' closing funds. In response to Mr. Trott, you talked about, in your testimony and in relation to his questions, education of the consumer. Could you also address, from a closer standpoint, a title company's standpoint, what best practices a typical closer or title company has implemented to protect customers' funds?

Mr. MENNENOH. Yes. Absolutely. First of all, we use encrypted email when we communicate with our consumers. We also have secure platforms where we can exchange information with our customers on a transaction. In terms of actually protecting the funds and what we do, our escrow trust accounts we have many security measures in place to make sure that anything that goes through there is watched very closely.

Most of our members do a three-way daily reconciliation of the account. We are reconciling our account every single day to make sure we see what activity is going through. We use Positive Pay for our checks. When we have an outgoing wire, we have a two-step authentication process. Once it reaches a certain level, there is a three-step process. To make sure that everything is being done, the wire instructions are correct, it is going to the right place. We take a number of steps like that to make sure that we are protecting the funds.

Mr. KUSTOFF. Some of the practices you have described, are those recommended by the American Land Title Association?

Mr. MENNENOH. Those are included in the ALTA best practices. Yes.

Mr. KUSTOFF. Do you have an opinion or would you have any knowledge what percentage of ALTA members follow those best practices?

Mr. MENNENOH. Honestly, I don't have a number for you. In traveling around the country, I can tell you that a lot of our members who are actively engaged in their State association or national association have implemented the best practices. But I don't have a number for you.

Mr. KUSTOFF. Again, I understand you don't have a number. For those entities that maybe have not adopted those best practices

standards, would the issue be cost, that is my first question. Can you elaborate on the difference between costs associated with cybersecurity for a small company and for a medium and large-sized company?

Mr. MENNENOH. Certainly. Yes. Cost is certainly an issue. It is costly to implement these things, particularly for a small company. Implementing these types of security measures is a good example, for my company, the amount of fees that we pay to our bank is in the tens of thousands of dollars per year to implement these various procedures and protections that we have in place just with the bank. It is a cost issue, and for small companies that is a big problem. But many of our members who are very responsible and want to do the right thing are very inadvertent.

Mr. KUSTOFF. Thank you. Ms. Schwartz, if I could. The collaborative efforts that have to be undertaken, if you will, by the financial sector and by law enforcement is incredibly important, I think we would all agree, in preventing and mitigating the risk that these cyber attacks pose.

In the event of a cyber attack, how quickly would your institution engage with law enforcement?

Ms. SCHWARTZ. Happily, my institution has not been the victim directly of a cyber attack. We have had—our members have been the victim from data breaches that have happened at the merchant level. We, would of course, cooperate fully should that unfortunate event happen. But we have DDoS protection, and we haven't had any direct attacks since 2015.

Mr. KUSTOFF. In those institutions, those members that would have attacks, are there law enforcement agencies that they typically go to, are they Federal, State, local? Who do they reach out to first and how do they collaborate?

Ms. SCHWARTZ. For our members, they would reach out to us, to say, What should we do? We would put everything in place, we could to protect them, whether it is the reissuance of cards, putting notification of fraud alerts on their accounts, best practices, webinars, telling them how they can put a freeze on their account through the credit bureaus.

Typically, because we cover the losses, as a financial institution, they are less concerned with reaching out, frankly, to law enforcement because we have covered them from those losses.

Mr. KUSTOFF. Thank you. My time is expired. Thank you, Mr. Chairman.

Chairman LUETKEMEYER. The gentleman's time has expired. Now we go to the gentleman from Kentucky, chairman of the Monetary Policy Subcommittee, Mr. Barr, recognized for 5 minutes.

Mr. BARR. Thank you, Mr. Chairman. Thank you for holding this very important hearing. I hear very regularly from both retailers and the merchant community back in Kentucky, in addition to community financial institutions that serve consumers in central and eastern Kentucky, about the problem of data security, of course, the Equifax breach is a warning to us all that this is a very large scope problem.

As we marked up the legislation last year to attempt to address this problem, the Carney/Neugebauer legislation, we got different competing stories from the various different actors that would be

affected by this. I kind of want to unpack all of that discussion here.

A community bank in Kentucky has told me that they have increased spending significantly over the last 18 months on data security. Why? Because they have seen the number of account takeovers triple. Meaning, scammers, through the use of personally identifiable information and security questions data try to gain access to an account by calling the bank and asking for addresses to be changed and new debit cards to be ordered. Et cetera.

These same community banks and credit unions tell me that they are spending a whole lot of money dealing with the fraud and reissuance of cards. What they talk about is the weakest link in the data security system. My first question to Ms. Schwartz is where do you view the weakest link to be?

Ms. SCHWARTZ. In the payment market, they are absolutely right. The weakest link is where the criminals are going to go, and frankly, it is at the merchant level at this point. Mission Fed spent over a million dollars in 2017 for data security. Many of the merchants have little or no protocol in place for things as simple as getting rid of old data or shredding or virus protection. It doesn't have to cost a million dollars. There is basic financial hygiene, if you will, that can be implemented at a reasonable cost, no matter what your size.

Again, going back to Gramm-Leach-Bliley, as a scaleable and flexible rule that does provide a nice framework for protecting important consumer privacy data, financial data.

Mr. BARR. Now, what would you say, Ms. Schwartz, to the kind of response from the merchant community that the breach notification legislation that we voted for in the last Congress would subject retailers to stringent bank-style security rules, whereas, banks or credit unions would be subject only to discretionary guidance?

Ms. SCHWARTZ. I don't think it is discretionary for us. It is our reputation. We are responsible, on the hook monetarily, and we are very, very heavily regulated. I think H.R. 2205, which I believe is what you are referring to, did a very nice job at providing a level playing field, because again, if you don't have the standards throughout the whole payment systems infrastructure, the criminals are going to find the weakest link.

Mr. BARR. Yes, I think, so community financial institutions in my district also would say that Regulation E forces them to pay when their customers are harmed, even though it is not their fault, when it is the fault of some other party. That is very understandable anxiety for those folks.

But let me just kind of continue to try to unpack this, because the merchant community will say that small businesses simply don't pose the same kind of risk because they are only dealing with a small category of vulnerabilities, namely, credit card information, not a range of other kinds of sensitive information.

What would you say in response to that?

Ms. SCHWARTZ. I would say in 2017 until the end of September, at my credit union alone, we have had 14,500 cases of reported fraud, costing us \$1.7 million, money that could have been better spent serving our members.

Again, basic financial hygiene of protecting sensitive data, updating virus protection, does not seem like an unreasonable standard for those merchants to have to follow in return for having a good business practice, a good name.

Mr. BARR. Yes. I am very sympathetic to your point of view, at the same time, I want to figure out a way forward, especially with those small businesses that are pushing back. Any help that you all can give us in terms of working with the merchant community to come—to work through these issues would be appreciated, because we clearly need a solution. I think all parties, to their credit, have supported passage of some kind of Federal data breach notification law to replace the existing patchwork.

I have run out of time so I will yield back.

Chairman LUETKEMEYER. The gentleman's time has expired. With that, we go to the gentleman from Georgia, Mr. Loudermilk, he is recognized for 5 minutes.

Mr. LOUDERMILK. Thank you, Mr. Chairman. I appreciate the panel being here. This is—being in the IT arena for 30 years, and 20 of that in the private sector, and prior to that being in the intelligence community, security is something that has been a grave concern of mine over the years, especially when I have been in Congress. It is something that we are going to be continually chasing.

One of the things that I emphasized on the businesses that I served in the IT industry, most of them small, medium size businesses, is it is impossible to protect yourself from a hack, from an intruder. The idea is, you make yourself a harder target than the other guy. That is sort of like the story of the two Georgians who went hiking in Alaska, one of them took a 357-magnum, the other took a pair of tennis shoes because they were afraid of bears. The guy with the gun said, you can't outrun a bear, why are you taking those? He said, I don't have to outrun the bear, I just have to outrun you.

That is really the idea that cybersecurity is making yourself a harder target than the risk that you propose. The other aspect of that is something that we held when I was in the intelligence community when it came to security is that you don't have to protect what you don't have. It deals with data retention, which Ms. Schwartz indicated earlier, especially with small businesses, is the amount of data that you are keeping. If you don't need it, you need to destroy it, which leads to an area that I have begun looking into.

I think that we, the Government, create a security issue ourselves by the regulations that we impose upon, especially the financial services industry, making these businesses obtain and maintain information for long periods of time that they really don't need.

Ms. Schwartz, can you opine in this? Is there data in credit unions, and especially small banks, that we require you to get that you wouldn't obtain, except for the Government is telling you to keep it?

Ms. SCHWARTZ. I am not going to argue with the fact that we have to maintain and submit an awful lot of data to our regulators. When we do a mortgage, in particular, there is more and more data points that are being collected and provided. That is absolutely

true. It has exponentially increased over the years as to how much we need to maintain, retain, and provide.

Mr. LOUDERMILK. OK. Mr. Bentsen?

Mr. BENTSEN. It is a very good question. A lot of data collected and held for regulatory mandates and submitted to our regulators is with no malintent, it was part of the process. But as we moved into this age, it is really something that we really need to think about. It is part of our principles as well, do you need it in the first place? How long do you need it? Who should have access to it? When you don't need it, how do you get rid of it so you eliminate the target in that response? That is my point with Consolidated Audit Trail, which is something that was not designed to capture PII, but does in the current design. It is designed to monitor market activity. You are creating this massive database with a lot of sensitive PII in there. The question needs to be asked, just like the industry asks itself, do we need that to accomplish the underlying goal?

Mr. LOUDERMILK. Exactly. Mr. Mennenoh?

Mr. MENNENO. A very simple example is many, many years ago the title industry was required by a regulation to collect information for the issuance of 1099s on real estate transactions. That means that we have to collect Social Security numbers so that we are effectively the watch dog for this, for the IRS, and this is something we have been forced into doing and we have to maintain that to prove that we have done what we are supposed to.

Mr. LOUDERMILK. I am also a member of the Science, Space and Technology Committee, and we have been looking into cybersecurity risks for 3 years I have been in Congress. I asked the Inspector General, not long after the OPM data breach, if you would rate the Federal Government's ability to protect data, our cybersecurity preparedness, on a simply elementary school rating system, what would you rate the Federal Government? His answer was a D minus. He said, it was only because of the minimal changes that were made in APM, I am not giving it an F. But, yet, we are continually having to provide to the Federal Government massive amounts of data on your customers.

That is why I keep addressing this is—maybe one of the theories we need to address that area of—the amount of data that you are required to obtain and maintain.

One last question. I see I am running out of time, Mr. Chairman, so I will yield back. Thank you.

Chairman LUTKEMEYER. The gentleman yields back. With that, we will go to the gentlelady from New York, Ms. Tenney, is recognized for 5 minutes.

Ms. TENNEY. Thank you, Mr. Chairman and thank you panel. This is a complex issue, and actually, I am not sure who to address these questions to. I was a former member of the New York State Assembly, and as we—I don't think it was the wisest move, our Governor decided to consolidate our insurance and banking industries into one big institution, Government institution, and then obligated many of our banks and our institutions to provide data, much like Mr. Mennenoh was talking about with the 1099 data for real estate closings.

I attended a cybersecurity event where a cybersecurity expert said, the worst place to reserve your data is in a Government entity. It is safer and better in banking institutions and financial institutions. As Ms. Schwartz cited, your reputation is on the line, and the incentive for you to protect that and be competitive in the marketplace is certainly much greater than Governments.

I know we are trying to get to the bottom of this. But toward that end, and I will address this to Ms. Schwartz initially. Can you tell us some way that we can help in Congress to minimize your—the requirement that you come up with data—extra data turned over to Government with confidential information, with some other way that you can protect it, and we can know with assurances that without that data getting into the stream, how can we protect it in some way?

Ms. SCHWARTZ. I think much of the data is requested with the best of intentions.

Ms. TENNEY. Exactly. We know they are good intentions, but getting hacked is certainly by somebody without good intentions.

Ms. SCHWARTZ. But we are very heavily regulated, very heavily examined. Most of the data would be available at examination time, without needing to be transmitted on a loan by loan or account by account basis. Other than—

Ms. TENNEY. You are suggesting that instead of turning the data over, as is sometimes required by say New York State, it would be sampling of data, as opposed to a full turnover of data.

Ms. SCHWARTZ. Or it could be a full turnover of data when the examiners are onsite. They can look at any anything they want while they are onsite without having to electronically transmit it.

Ms. TENNEY. That sounds like a great option. I appreciate it. Mr. Mennenoh or Mr. Bentsen, would you like to comment or—

Mr. BENTSEN. I agree with that. A situation we have now is about what is known as penetration testing, and this is something that firms do to test their own defense system, and they may do it with their own teams, or they may bring in an outside vendor to do it. Certain regulators in the U.S. and around the globe have wanted to create a mandate around using third party vendors, and the industry has become concerned, because in doing this you are kind of giving the keys to the castle to an outside party.

Then in reporting to our regulators, if you have to report the whole road map, you are handing the keys over, again, to an outside party. We completely agree from the standpoint of, come in, sit down, look at the data, we will walk you through it, you can tell us what you don't like, or what you want us to change, but let's be very careful about spreading that all over the place, again, with the best of intent. Let's not create targets unnecessarily.

Ms. TENNEY. I appreciate that. Maybe you could comment—I agree a hundred percent. I think that, obviously, Government is well-intentioned, but it is unpredictable. The people in power change, the people in positions change, and so you have—it seems to me the data is just drifting across unsafe and insecure regions. But maybe you can comment on that as well, Mr. Mennenoh.

Mr. MENNENOH. I would agree that it is—we are being asked for information, certainly more frequently. Many States in our indus-

try are regulated, they do have audits and those things that are being done. Certainly, an onsite audit of paper is a lot easier to secure than a digital audit that is being sent all over the place. It is troubling.

Ms. TENNEY. Thank you very much. I appreciate your testimony. I yield my time back. Thanks so much.

Chairman LUETKEMEYER. The gentlelady yields back. We will now go to the gentleman from California, Mr. Royce.

Mr. ROYCE. Chairman, thank you. Thank you very much. I thank the panel here. I was looking through my notes, and every 2 years, like clockwork here, we hold a hearing and it follows always a major breach in consumer data by a U.S. company. Here we are again, and the massive Equifax breach exposed the personal information of 150 million consumers. Before that we had Anthem, we had Yahoo, we had Home Depot, and of course, Target, and even the Federal Government's Office of Personnel Management, as the Chairman of Homeland Security reminds me, since his data was stolen.

These breaches have made the headlines, and then the hearings follow, and then, of course, outside of Gramm-Leach-Bliley, we have failed to pass legislation into law that puts in place national standards for data protection and national standards for breach notification. We have failed to do that on our part here.

To be very clear, the Committee has acted, this Committee has acted repeatedly. We have passed legislation over and over again. But it is high time that we put any policy differences aside and enact a law that serves the American people. I know the chairman—I want you to know, Chairman, I stand ready to work with you. I suspect you will be the author of the bill. To do this, we have to convince our colleagues as we move it out of committee, which certainly you will, to take this seriously with respect to getting it over in the Senate, and then things will become more complicated. But we have to convince the Senators to move this legislation as well.

I would like to ask Ms. Schwartz a question. Community financial institutions are often the face of data breach for your customer, although not necessarily the cause. In your testimony you cite a July 2017 NAFCU member survey. The estimated cost of data breaches in 2016 was \$400,000 per credit union.

Credit unions in California have been very hard hit. The target breach cost the Credit Union of Southern California \$35,000. The Home Depot breach costs Schools First Federal Credit Union in my area, they are in Orange County, \$700,000, with a 65 percent increase in card fraud. Coast Hills Credit Union watched \$100,000 in fraud hit their system in 5 minutes because of that same breach.

Do these numbers ring true for your credit union in San Diego as well?

Ms. SCHWARTZ. Sadly, absolutely. In 2017, we had 14,500 separate reported cases of fraud. It has cost my credit union \$1.7 million so far this year. The holiday season is typically also a fraud season, so we expect to see more. Over \$6 million since 2003 in fraud losses.

Mr. ROYCE. Six million for your membership. How much reimbursement of your costs is covered by contracts with vendors and payments networks?

Ms. SCHWARTZ. Pennies on the dollar. The fraud losses I mentioned are simply the hard costs. There is also staff costs. The cost of us implementing security measures. The cost of educating our members, educating our employees. There is both the hard dollar costs and the soft costs. The remuneration is minimal.

Mr. ROYCE. Do you think there is a better way to allocate financial responsibility for breaches in order to incentivize companies to better secure data?

Ms. SCHWARTZ. Absolutely. We very much support a level playing field. H.R. 2205, which was introduced in the 114th Congress, provided that, Gramm-Leach-Bliley is a dynamic, scaleable, flexible tool that should apply to largest and smallest. It applies to small credit unions, it could apply to small merchants.

Mr. ROYCE. Let me get a quick question in here for Ken, if I could. As I mentioned in my opening, failures in cybersecurity systems have occurred in the private sector and in the Government—within the Government. Representing an industry that shares an enormous amount of sensitive customer data with regulators and other agencies, do you feel the Government is doing enough to shore-up its own systems to protect against cyber attacks?

Mr. BENTSEN. Thank you for the question, Congressman. This is an ever growing threat. I think the Government increasingly understands that, and we are engaged in dialog with our regulators about how we protect the data when we hold it, and the best practices that we use. The Treasury has been leading an effort to look at how they protect the data that they collect. This is an emerging issue that I think has gotten the spotlight with everything going on.

Mr. ROYCE. Thank you. Thank you, Mr. Chairman.

Chairman LUETKEMEYER. The gentleman's time has expired. With that, we go to the gentlelady from Utah, Mrs. Love, who is recognized for 5 minutes.

Mrs. LOVE. Thank you. Thank you for being here. I have a question that I want to address, Ms. Schwartz, you mentioned in your testimony that credit unions left often cleaning up the mess when another institution suffers from data breach. Institutions such as retailers that aren't subject to a data security structure like the Gramm-Leach-Bliley, you have written this in your testimony.

Could you summarize for me what that mess looks like for credit unions like yours, and what kind of costs are involved in that?

Ms. SCHWARTZ. To scale it—my credit union has issued about 280,000 credit cards to our members. Over the past few years we have reissued 146,000. A significant number of our members have been impacted, some more than once, many more than once.

Mrs. LOVE. Right.

Ms. SCHWARTZ. They don't always understand where the breach happened, most particularly because often we can't tell them where the breach happened. They tend to think that the financial institution is the responsible party, when we have not been.

Mrs. LOVE. When you are reissuing over half, what does that cost look like?

Ms. SCHWARTZ. Just for fraud itself was \$1.7 million for us so far this year, through September 30. We anticipate it will be well over \$2 million just for the fraud occurrences. Reissuance of the cards depends on the type of card and whether the PIN was compromised. It ranges between \$2 to \$6 per PIN, just for the hard cost. Then, of course, there is the soft cost of answering all of those member questions.

Mrs. LOVE. Right. OK. Are you able to break down those numbers by different types of breaches, such as by source?

Ms. SCHWARTZ. If it is a huge breach, we will typically go back and take a look and be able to determine. Oftentimes, because there are so many different cases, 1,400 different breaches is not practical for us to spend staff time to try and tie back every single bit. We are financially responsible to the members, we reimburse them, and then we move on to the next.

Mrs. LOVE. OK. You also mentioned that one of the vulnerabilities in sectors beyond bank and credit unions is lack of examination for compliance with data security standards. You specifically mentioned that credit bureaus, like Equifax, are not examined for compliance with the GLBA. How big of an impact do you think this makes, and how should compliance be insured?

Ms. SCHWARTZ. I think it clearly makes a huge difference. If they had followed the Gramm-Leach-Bliley Act requirements, it is very possible the breach wouldn't have happened. The patch would have occurred in a more timely manner and the opportunity for the fraudsters to gather that data simply would not have been there. Absent a regulatory examination to ensure compliance, I don't think it happens.

Mrs. LOVE. Would it be fair to say that if institutions or the credit bureaus, like Equifax, had as much skin in the game, in other words, if they were held responsible financially for these breaches, that you would see fewer of these things happening?

Ms. SCHWARTZ. No question.

Mrs. LOVE. OK. I have a few more minutes. There was a part where you pointed out in your testimony that the breach may never come to fruition if an entity handles sensitive information, limits the amount of data collected on the front-end and is diligent in not storing sensitive personal data and financial data in their own systems.

Do your consumers even know, for example, if they are sitting at their computers shopping online, what happens to their data, especially the data that they are being asked to supply?

Ms. SCHWARTZ. I think consumers are becoming more educated on this, but I think they are more concerned with the transaction than what is happening behind it. I am sure that they don't realize that many merchants can store that data for an unlimited period of time, even though they might not have shopped at a certain merchant, that data is going to linger out there forever.

Mrs. LOVE. In other words, sitting at their computer, they probably feel like there is some vulnerability there, but they have no idea that the vulnerability lingers way past the time that they are actually sitting on the computer.

Ms. SCHWARTZ. Exactly.

Mrs. LOVE. Over 1.4 million Utahans were affected by the Equifax breach, and as information is growing and changing, it is something that is incredibly concerning. I think that this is an example of how we need to have institutions that are holding onto this data have some skin in the game, that they know that they are absolutely responsible for those breaches, also. I think that where a lot of responsibility is given, you have to make sure that you take care of that responsibility carefully. Thank you for your testimony.

Chairman LUETKEMEYER. The gentlelady's time has expired. With that, we go to the gentleman from North Carolina, Mr. Pittenger, is recognized for 5 minutes.

Mr. PITTINGER. Thank you, Mr. Luetkemeyer, for hosting this hearing. I really appreciate each of you all being with us today, your input is extremely valuable.

In North Carolina we have had a significant impact with 1.1 million North Carolinians' personal data stolen in various security breaches since 2015, up from 300,000 in 2014. The Equifax had an impact of 5 million North Carolinians. It is a clear indication of the concerns that we have with data and security concerns, as well as congressional action that needs to be provided.

With that in mind, I would like to ask you, Mr. Bentsen. In your own statement you referenced that we need to have a combination of activities that relies on strong defenses, information sharing, mitigation, and recovery planning.

To the point of information sharing, Mr. Mierzwinski conveyed that you cannot bifurcate data sharing and privacy issues. How would we mitigate the privacy concerns with the need that we truly do have for greater data sharing?

Mr. BENTSEN. That is a very good question. We are interested in information sharing, not only with the industry being able to share with the Government, the Government being able to share with the industry when there is a certain attack, but also to be able to share not data as much as sharing the types of attacks that are occurring across the sector.

Mr. Loudermilk talked about this in the past, one of my defenses is having somebody else get attacked so they are not coming after me. What we have tried to do in the financial services industry is to be able to spread the information across the sector quickly if a certain type of attack is occurring so that others can recheck their defenses against that or their resiliency efforts against it. We think that is really important.

At the same time, the industry feels very strongly, not only about our legal obligation with respect to protection of privacy, but as Ms. Schwartz says, our reputational obligation to our clients. It is a highly competitive industry, and if we are viewed as not protecting our clients' data, they are going to go somewhere else. It is a spot-on question.

Mr. PITTINGER. Recognizing this need, how would you frame legislation? How would you advise us to address this concern?

Mr. BENTSEN. We were not part of the legislation referenced from the 114th Congress, and obviously, you have parties on all sides who have—or interests on all sides who have legitimate concerns about that. Data breaches are just one component of this, but it is

a huge component. It maybe has the biggest retail aspect in some respects, and a huge market failure would have a huge retail impact as well.

This is an emerging issue that is only going to get worse. It is not going to get better. It is something where policymakers, such as Congress, are really going to have to dig in and bring the parties together, and by that, the interests—political parties perhaps as well, but the interests together to really see how can we look into the future, because we are also going to see technology use increase. Technology is a good thing, it has improved efficiencies in the economy, it is only going to do more of that. But it is going to create new risk, and we need to be in front of those going forward.

Mr. PITTENGER. Thank you. Mr. Mennenoh, you stated in your remarks that policymakers should consider better ways to use both the SARS reports, and IC3 data to better detect accounts used by these criminals.

Give us some examples of better ways that we should be employing?

Mr. MENNENOH. That is a good question. I don't know that I have a clear answer for you on that without having the staff help me with that. But, certainly, I would say being able to provide information to all of the parties in the real estate transaction, the different industries that are involved in terms of where these problems occur, how they occur, and the warning signs, if you will, to detect them, to try to prevent them. I don't know that I can help you further than that.

Mr. PITTENGER. Ms. Schwartz, quickly, you stated that Congress needs to modernize data security laws to reflect the complexity of the current environment, insist that entities collecting and storing personal financial information adhere to strong Federal standard in this regard.

How would you modernize those laws?

Ms. SCHWARTZ. I think Gramm-Leach-Bliley does provide a good model because it is scalable and flexible. I think it can apply to small and large, and it provides some basic guidelines that ensure sound practices.

Mr. PITTENGER. Thank you. My time is expired.

Chairman LUTKEMEYER. The gentleman's time has expired, and we are out of questioners. All of you on the panel are freed up here at this moment. Thank you for being here today.

Just a few closing thoughts. We are a very data driven society. I am a big baseball fan. Even data drives the baseball games. I have been watching the World Series, and they talk about this batter can hit this pitch in this area and you have shifts on the defense to where you go, and they match up pitchers between the batters. It is all back to data, data, data, which is great to a certain extent.

But I think, Mr. Bentsen, your last comment there was very succinct when you say, with all this data comes new risks, and how do we protect ourselves against those risks. I think that is what we are concerned about today, as we see these breaches continue. The gentleman from California a minute ago, Mr. Royce, said, here we are again. Here we are again.

We have to figure out how to put some solutions on these problems, and hopefully your information today will help us. I think we need to look at notification. To me, that is a big issue. How do you make sure that the public, whose information that you as a business—or Government have, how do you notify them when you have been breached so that there is a level of trust there, so that you can give those folks notice that they can get themselves in a position where they can protect themselves.

Who assumes the liability whenever there is a breach? To me, that is a big question. I think Mr. Barr asked that question a while ago. We need to figure out where that stands, because I can tell you there are some businesses, I think, one of them, I think maybe it was Andy here a minute ago, made the same comment with regards to businesses, who through no fault of their own, it is costing them thousands and thousands of dollars as a result of breaches. This has to go back to entities that caused the problem and they have to be held accountable.

We are looking for help, we are looking for answers. We are going to continue to work with you on these issues. We certainly appreciate your being here today and all of your input, and again, as I said, welcome your input back to us on other concerns or questions that may have come up during the discussion.

The Chair notes that some Members may have additional questions for this panel, which they may wish to submit in writing. Without objection, the hearing record will remain open for 5 legislative days for Members to submit written questions to these witnesses and to place their responses in the record. Also, without objection, Members will have 5 legislative days to submit extraneous materials to the Chair for inclusion in the record.

[Whereupon, at 3:45 p.m., the subcommittee was adjourned.]

A P P E N D I X

November 1, 2017



Written Testimony of
Kenneth E. Bentsen, Jr., President and CEO, SIFMA
before the U.S. House of Representatives
Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit
Hearing entitled "Data Security: Vulnerabilities and Opportunities
for Improvement"
November 1, 2017

Chairman Luetkemeyer, Ranking Member Clay, and members of the Subcommittee, thank you for giving me the opportunity to testify today on the important topic of cybersecurity and data protection. The Securities Industry and Financial Markets Association (SIFMA)¹ represents hundreds of banks, broker-dealers, and asset managers who collectively are dedicated to protecting their systems and more importantly, their clients' data, from cyber-attacks. There is likely no greater threat to financial stability than a large-scale cyber event and so SIFMA and its member firms are deeply committed to improving our sector's cybersecurity resiliency and working with our government partners to protect the broader economy. Our members have invested tremendous monetary and human resources to develop and implement cyber defense and recovery mechanisms and we welcome the opportunity to discuss the progress made and challenges identified.

The cybersecurity landscape is complex with a wide array of hostile actors, including criminals seeking financial gain, nation states engaged in corporate espionage or worse, and terrorist groups seeking to disrupt markets and create fear. Cybercrime is now a bigger criminal enterprise than the global narcotics trade. The financial services industry is a top target facing tens of thousands of attacks each day. While data breaches of customer information dominate headlines, and are an appropriate concern for policymakers, a major cyberattack on critical financial market infrastructure or one that destroys records and financial data, is a risk with a potentially far larger impact on the economy.

While regulation and supervision of cyber preparedness has an important role in the collective cyber defense effort, the emergence of many regulations from multiple regulators may lead to a suboptimal balance of industry resources devoted to compliance versus security.

October marked National Cybersecurity Awareness Month, a prime opportunity for the industry and regulators alike to have assessed how cyber defense and response policies and protocols can be improved to protect our nation's critical infrastructure, including the financial markets. Enhanced harmonization of regulatory standards and supervision would improve the efficient use of critical

¹ SIFMA is the voice of the U.S. securities industry. We represent the broker-dealers, banks and asset managers whose nearly 1 million employees provide access to the capital markets, raising over \$2.5 trillion for businesses and municipalities in the U.S., serving clients with over \$18.5 trillion in assets and managing more than \$67 trillion in assets for individual and institutional clients including mutual funds and retirement plans. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA). For more information, visit <http://www.sifma.org>.

cyber resources. In simple terms: financial institutions shouldn't have to devote limited resources to redundant regulatory and supervisory requirements at the expense of actual security-based activities.

But it is important to recognize that no single actor – not the federal government, nor any individual firm – has the resources to protect markets from these threats on their own. It is critical that we establish a robust partnership between industry and government to mitigate cyber threats and their impact. The industry's resiliency will not be fully effective without the government's help, and vice versa.

Make no mistake, both the industry and our regulators are in complete agreement that cyber security and resiliency are and should be a top priority. And our collaboration with regulators on the matter has never been greater. Cybersecurity is truly a shared objective where the interests of the government and private sector are fully aligned. We are all targets and the industry remains vigilant to confront this risk every day.

For our part, the securities industry is constantly working to improve cyber defenses, resiliency and recovery through massive monetary investment in technology and personnel, regular training, industry exercises, and close coordination between the financial sector and the government, including our regulators. This is a C-Suite and Board-level issue and has been a top industry priority for several years. A strong collaboration between the government and private sector is key to success. Continued work to streamline and coordinate regulation would strengthen this partnership and help to better protect investors and the markets.

Today, I would like to outline some key areas of focus for SIFMA's members. While this list is not exhaustive of our cyber agenda, it may be timely and of interest to the Subcommittee. SIFMA's top priorities include: protecting customer data; coordinating cyber regulations across government; and ensuring that information shared with third-parties is adequately protected. I will also speak on SIFMA's efforts to prepare industry for cyber eventualities through industry-wide exercises that allow firms to simulate responding to attacks.

Data Protection

In recent years there have been an increasing number of highly visible data breaches, affecting billions of customer records. These breaches have targeted a broad range of organizations, from retailers and financial institutions to Federal and state governments and regulatory bodies. A recent study found that in the first half of this year, 918 data breaches resulted in a total of 1.9 billion records being accessed.² These attacks demonstrate that any public or private sector institution which holds sensitive information can, and indeed will be, a target of malicious actors. The development of sound practices by all members of the financial sector is critical. We have moved into a new era that requires us to be more tactical in our understanding of the data management lifecycle and what it might mean if that chain is broken by a malicious actor. All of us have a shared responsibility to protect sensitive information. Our members, clients and the public all expect our standards as a sector to be higher and our judgment to be sound.

Working with our members, along with our sister trade associations, SIFMA has recognized a number of best practices for the protection of sensitive data in the financial services sector. These practices draw on the experience of our member firms and their own policies and procedures, as well as industry standards such as the National Institute of Standards and Technology's (NIST) Framework for Improving Critical Infrastructure Cybersecurity.³

The experiences of our members show the importance of developing a culture and practice dedicated to the protection of sensitive data including an investor's personal identifiable information or "PII." This requires focus across the entire ecosystem, extending from when the decision is first made to collect a given piece of data through its eventual destruction when no longer needed. At each of these stages, organizations must be committed to best practices to ensure that their systems and processes are protected.

Data protection begins with firms taking a risk-based look at what information they collect – do they have a business or regulatory purpose that requires them to hold this information? If sensitive

² <https://blog.gemalto.com/security/2017/09/21/new-breach-level-index-findings-for-first-half-of-2017/>

³ <https://www.nist.gov/sites/default/files/documents/cyberframework/cybersecurity-framework-021214.pdf>

information like social security numbers is not directly relevant and necessary, firms should refrain from collecting it.

Once firms have collected sensitive data, they should ensure that they have controls in place to protect it while it is being used or stored. This includes ensuring that access to sensitive data including investor information is restricted only to authorized users who need it to perform their jobs – and making sure that as individuals change their roles and responsibilities, their access to sensitive information is updated as well. Keeping access to this data focused only for those who need to use it helps reduce the potential points of risk. Firms should also have policies such as data loss prevention controls, multifactor authentication to control access to sensitive data, as well as maintain a detailed audit trail of how sensitive data is handled while in possession to identify any weaknesses or vulnerabilities.

In addition to protecting data within the four walls of their organization, firms should be mindful of the associated risks when they share sensitive information externally. Firms also need to understand the security controls in place at any organization they share sensitive information with, and ensure that the process of transferring information is secure, such as through encryption. Firms should also work to reduce risk by destroying sensitive data once it is no longer needed.

To further protect sensitive data, firms should also draw on the range of available information security, cybersecurity tools and expertise where appropriate – including vulnerability scans, penetration testing (e.g. manual ethical hacking, dynamic analysis), timely remediation of weaknesses once they are identified, robust security training for their teams, and procedures for notification of breaches.

This focus on data protection also extends beyond securities firms themselves to encompass other entities with whom we share information. The risks posed by third parties have been recognized by regulators in the U.S. and internationally, such as the Office of the Comptroller of the Currency (OCC)'s release on Third-Party Relationships: Risk Management Guidance.⁴ To understand and mitigate these risk, firms have extensive vendor management and third-party risk assessment

⁴ <https://www.occ.gov/news-issuances/bulletins/2013/bulletin-2013-29.html>

programs. To help firms better understand the security environment at their third parties, SIFMA worked with the AICPA to help develop audit-based cyber attestations, based on NIST and other industry standards. As a highly-regulated sector, our members provide a tremendous range of sensitive information, including that of their retail and corporate clients, with regulators in accord with their supervisory mandates. This data is subject to protection and standards shaped by the Federal Information Security Modernization Act (FISMA), and given the ever-increasing risk, our sector is engaged in important dialogue with our government partners to ensure and enhance protections across the board.

Financial firms and regulatory agencies share a common goal in securing and protecting the data entrusted to them by clients and financial institutions. This information can include both personally identifiable information such as social security numbers, dates of birth, or other information provided by retail clients, as well as corporate data and intellectual property which institutional clients entrust to the financial services industry.

Consolidated Audit Trail (CAT)

As the Securities and Exchange Commission and self-regulatory organizations (SROs) move forward with the development of the Consolidated Audit Trail (CAT), SIFMA member firms want to ensure that the development of the CAT does not introduce new data protection risks. The CAT system was developed in response to the 2010 “Flash Crash” to improve regulators’ ability to monitor market activity and identify manipulation and other illegal activities, but as currently designed, the CAT could also be a gateway for cyber criminals to access confidential trading information and the personal information of tens of millions of retail investors.

Once complete, the CAT will be the world’s largest data repository for securities transactions, and one of the world largest databases of any type. Every day the system would ingest 58 billion records – orders, executions and quotes for the equities and options markets – and would maintain data on over 100 million customer accounts and their unique customer information. This data would grow to an estimated 21 petabytes within 5 years – the equivalent of over ten times the content of all U.S. academic research libraries, in a single database.

The current National Market System plan, developed by the exchanges and FINRA and approved by the Securities and Exchange Commission, raises serious concerns around data protection and the ability to confidently secure the critical information it will contain. One of our top concerns is that the CAT will hold massive amounts of personally identifiable information on retail investors who trade in the U.S. securities markets. The current CAT plan requires reporting firms to provide a significant amount of sensitive customer information, including name, social security number, and address. The CAT will also hold sensitive trade information, which could be used to reconstruct proprietary trading strategies. The database will provide regulators with the ability to aggregate information from all broker dealer and exchange CAT reporters. This information will be held in a single database that creates a high value target, and bad actors will have a strong incentive to find the weakest link to gain access. While our concern existed before the recent breaches, many stakeholders remain skeptical that the CAT, as currently designed, will be able to protect the massive amount of sensitive PII for every investor in America.

Importantly, just as the industry should and does consider whether sensitive information needs to be collected and retained for a particular purpose, so too does the case need to be made that PII is required to be collected and reside inside the CAT for effective surveillance.

The range and scale of data stored in the CAT alone would raise data protection concerns, but the current proposed policies for securing and accessing the database are not adequate. The NMS plan which lays out requirements for the CAT system requires that the system support a minimum of 3,000 users. Twenty-two different SROs as well as the SEC will have access to the CAT trading data. Under this configuration, it will not be enough to secure data held within the CAT system itself. Rather, every user with access to bulk downloads of sensitive data, across every participant SRO, will need robust security protections as well.

Despite these serious data protection concerns, the CAT technical specifications that have been released to date include alarmingly few details on data security and protection. In addition, SIFMA is concerned that an unreasonably tight timeline, which is based on arbitrary dates as opposed to the proper time needed for effective development, will not allow for adequate time to implement the necessary cybersecurity and data protection measures.

Given the sensitivity of the information held by the CAT on securities markets and retail investors, we believe that the design and development process of the system needs to ensure it is completely secure against breaches and data loss – and the system requirements and development timeline should be oriented to make sure this critical goal is achieved.

Importance of Regulatory Harmonization

Over the past two years regulators in the U.S. and around the world have proposed or finalized over 30 new cyber rules and regulations applicable to the financial services industry. While regulations can help raise expectations and define strong standards for market participants, the volume of regulations have resulted in requirements which are sometime overlapping, duplicative and conflicting.

Consider that for the financial services industry there are no fewer than 11 federal agencies that impose some form of cybersecurity requirements. This is in addition to individual states' requirements and those of self-regulatory organizations such as the Financial Industry Regulatory Authority and the National Futures Association. These rules and guidelines are further layered with standards developed by the National Institute of Standards and Technology and the International Organization for Standardization, which guide financial institutions in setting cybersecurity standards and measuring the adequacy of cybersecurity programs. Large financial institutions may also be subject to additional or different cyber regulations in each region where they conduct business.

As the number of different regulations increase, so to do the resources firms need to spend to demonstrate compliance. When the process of rule writing at agencies is not coordinated, the risk of different definitions, measurement standards, and technical requirements proliferate, creating administrative burdens for firms. Some large firms report that approximately 40 percent of their corporate cybersecurity activities are focused on compliance rather than security, where their time and resources could be better spent building even stronger defenses and better resiliency and recovery.

In recognition of the cyber threat to the financial sector, a coalition of financial services trade associations and the Financial Services Sector Coordinating Council (FSSCC), working with SROs, state regulatory agencies, and members of the Financial and Banking Information Infrastructure Committee (FBIIC) agreed to create forums to discuss various guidance, tools, frameworks, regulations and examination processes, built around the NIST Framework.

Regulators could help enhance defense and resiliency by establishing a unified cyber assessment framework and common set of controls across financial services regulatory bodies. The use of consistent language and terminology in regulations, guidance, rules and examinations would go a long way in promoting efficient cybersecurity spending. The cybersecurity standards developed in 2014 by the National Institute of Standards and Technology could form the basis of this common framework.

To their credit, regulators should be recognized for making strides towards harmonization, including the formation of a Regulatory Harmonization Working Group. The industry also welcomed the President's May 2017 Executive Order calling for a comprehensive review of cybersecurity efforts across all government agencies.

In parallel with the joint-trades effort, SIFMA and our affiliated non-U.S. organization have advocated for the global use of the NIST Framework and the industry is developing a financial sector version of NIST to encourage global adoption.

This harmonization of regulations and a common framework is essential to simplify the process of compliance and allow financial institutions to dedicate the right resources to protecting their institutions and securing sensitive data.

Penetration Testing

As firms and regulators look to improve their data protection and cybersecurity programs, many have recognized the value of penetration testing, as previously mentioned. Penetration testing allows firms to evaluate their systems and the controls that protect them, to identify and remediate vulnerabilities, and use these findings to strengthen their infrastructure against current cyber threats.

Regulators and supervisors internationally have also shown increasing interest in incorporating penetration testing into their cybersecurity oversight programs. This has led to the creation of multiple regulator-guided pen testing initiatives.

Despite the value of penetration testing in identifying vulnerabilities which firms can then correct, duplicative regulator-initiated tests may unintentionally increase risks to the financial services institutions. These risks could include:

- Damaging firms' production information security environments;
- Sharing of firm's sensitive test results data with third-parties increases the risk the firm will lose control of that data; and
- Forcing firms to spend more time on compliance and less time developing defensive measures to protect the organization's infrastructure.

Beginning in the first-quarter of 2017, SIFMA, working with its regional partners the Association for Financial Markets in Europe (AFME) and the Asian Securities Industry and Financial Markets Association (ASIFMA), organized through the Global Financial Markets Association (GFMA) led a global advocacy campaign to address the impacts of penetration testing on the safety and security of the financial sector and the need for a scalable sustainable way forward.

Our ideal end-state for this initiative is for regulators and supervisors to permit firms to test internally, or use external testers of their choosing. To ensure the quality of these tests, a firm's primary regulator would be involved in the scoping and scheduling of tests, and firms will provide regulators with confidence that tests are conducted by accredited certified professionals. Test results will not leave the subject financial institution; the full results can be viewed in-house at the firm by their primary regulator, with a summary of the results available to other regulators.

SIFMA and our affiliated organization have created a draft framework and white paper to outline a global firm-led testing framework to recommend best practices for conducting penetration tests. In this framework, we recommend principles that penetration testing regulations should provide primary regulators the ability to guide penetration testing programs at a high level, with common scenarios, scheduling and scope of testing activities. Regulators would also have transparency into

testing process and governance for both regulator-driven and firm-driven testing, as well as assurances that identified weaknesses are properly addressed. Furthermore, it would ensure testing activities are conducted in a manner that minimizes operational risks and enforces strict protocols for handling test findings due to the highly sensitive nature of this information.

Insider Threat

One of the greatest threats to our members' cybersecurity comes from within the firms – either current or former employees or others who have access to the firm's data. With the computerization of firm systems and assets, attacks can now be launched on a larger and more destructive scale than ever before. Insider attacks on firms' electronic systems can result in financial and intellectual property theft and the loss of sensitive client information, as well as firm-wide disruption to internal systems and customer operations. A recent Data Breach Investigation Report from Verizon shows that nearly 20% of breaches are caused by insiders and that almost 90% of breaches were motivated by financial gain or espionage.⁵ Preventing and detecting insider attacks, is essential as insiders often look to capitalize on their familiarity with firm systems to instigate attacks and compromise data without attracting notice. A systemized, targeted program is therefore necessary to mitigate the insider threat.

While insiders take advantage of weaknesses in technical systems, insider threats are, at their core, a human issue. Cybersecurity defenses focused on monitoring employee activities may prevent some attacks from causing significant harm to an organization. Human intelligence, monitoring and managerial oversight are necessary to identify the potential warning signs of insider activity and the appropriate method to intervene before an attack occurs. An effective insider threat program uses both cybersecurity defenses and intelligence personnel to detect and contain insiders who pose a risk to the firm and mitigates the risk through administrative, investigative, technical or disciplinary safeguards and responses.

SIFMA works to support firms as they develop their insider threat prevention programs – by building dialogue between our member firms and the public sector, academia, and technology firms,

⁵ http://www.verizonenterprise.com/resources/reports/rp_DBIR_2016_Report_en_xg.pdf

benchmarking of best practices, and developing best practice guidance to help firms build out a robust insider threat management program and to understand the legal context that shapes what is permissible.

Exercise Programs

As firms continue to develop their cybersecurity and data protection programs, we believe that sector wide exercises are a critical tool to help firms and regulators exercise their playbooks, learn to work together, and continue to find opportunities to improve their preparation and training. The lessons and experience firms develop during exercises help make themselves more secure and develop the muscle memory needed to quickly respond in the event of an actual cyber incident.

SIFMA has organized a series of sector-wide cyber exercises since 2011. These “Quantum Dawn” exercises have provided a forum for firms, regulators and law enforcement to exercise their playbooks, work together to respond to simulated cyber incidents, and identify opportunities to improve. With scenarios ranging from attacks on the equity markets to clearing and settlement disruptions to data breaches, these exercises have helped the industry learn and develop their capabilities. The latest exercise in the series, Quantum Dawn IV, will focus on exercising the industry’s ability to respond and recover from a targeted systemic cyberattack affecting multiple financial institutions, and how firm, sector, and government playbooks would support this process. The exercise will bring together nearly 60 financial services firms, exchanges, and utilities.

SIFMA and its member firms have also participated in a public-private exercise program, the Hamilton Series of cyber exercises, which brought together firms, trade associations, and U.S. government agencies to better prepare the financial sector to address the risks and challenges presented by significant cybersecurity incidents. The exercises range from regionally-focused events among small and medium-sized companies to cross-border tabletops, to sector-wide exercises. These scenarios examined impacts across different segments of the financial sector, including impacts to equities markets, depository institutions, payments systems, liquidity, and futures exchanges. The lessons learned from these exercises have helped the industry and our government partners identify what new initiatives would be most effective in continuing to improve the

industry's cyber and data protection policies, and where we can work together to help protect each other and our clients.

Sheltered Harbor

While the industry is committed to securing the sensitive data it has been entrusted with, we also plan for all contingencies including potential successful cyber-attacks. As part of regular joint government-industry exercises, we determined the need to develop a system to provide for the restoration of customer data when records are erased and systems compromised. The industry has organized a program called "Sheltered Harbor" to give the sector a protocol to safely secure retail customer demand deposit and brokerage accounts off site or off line in a standard recordable format.

Firms participating in Sheltered Harbor will be able to securely store and reconstitute their end of day customer account information, through a service provider or other firm, if they are unable to recover from a cyber incident in a timely fashion. All participating institutions, on a regular basis, will make a copy of the consumer's end of day account data in a standard format, which enables the restoration of accounts in the event of a major outage. The account data is archived in a secure data vault that is protected from alteration or deletion. The data will stay intact and accessible if needed - exactly as when it was archived. Sheltered Harbor is expected to be fully operational in 2018. Sheltered Harbor further aligns and compliments a joint securities industry regulator effort to ensure customers remain connected with their assets should a broker dealer experience financial difficulty through a swift transfer of that broker dealer's customer accounts to another broker dealer, and the subsequent reestablishment of the client relationship.

Conclusion

Effective cybersecurity will be in a state of discussion and improvement for years to come. That security is a combination of activities that relies on strong defenses, information sharing, mitigation and recovery planning. It can only be accomplished through constructive dialogue and engagement among the private sector, policymakers, and regulators. Much work has been done but as this

testimony lays out, there is much more work to come. SHMA and its members stand ready to do their part.

**TESTIMONY OF DANIEL D. MENNENOH ITP, NTP
PRESIDENT, H.B. WILKINSON TITLE COMPANY, INC.
ON
DATA SECURITY: VULNERABILITIES AND OPPORTUNITIES
FOR IMPROVEMENT
BEFORE
THE HOUSE FINANCIAL SERVICES COMMITTEE
SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

WEDNESDAY, NOVEMBER 1, 2017
WASHINGTON, D.C.**

Chairman Luetkemeyer, Ranking Member Clay and members of the subcommittee, my name is Daniel Mennenoh. I am President of H.B. Wilkinson Title Company, a title insurance agency headquartered in Galena, Illinois. I have been in the title insurance and settlement business for nearly 36 years. I purchased the company from my father. My wife and I have operated the company together for 20 years.

H.B. Wilkinson has 28 employees and has offices in seven counties, the most populated of which is Rock Island, which includes the Quad-Cities and has a population of approximately 150,000. We close about 70 real estate transactions a month or roughly 800 a year. By industry standards we are considered a large title company. The average title agency has less than five employees and revenue between \$250,000 and \$499,000 annually.

For the past year I had the honor of serving as the President of the American Land Title Association (ALTA). ALTA is the national trade association representing more than 6,300 title insurance companies, title and settlement agents, independent abstracters, title searchers, and real estate attorneys. ALTA represents many small businesses that serve their local communities and operate in every county in the United States.

One of my favorite responsibilities serving as ALTA president was traveling the country to meet with members of the association and hearing what was happening in their businesses and local markets. In those conversations, the one topic that always topped the list of concerns for title professionals was data security and the growing threat of criminals trying to steal our customers' closing funds. These small business owners were not just worried about the future of their business but also the threat to their customers potentially losing their life's savings.

With the spike in security incidents and fraud, the title industry has spent millions to protect its customers' money and data. Like other financial companies, members of the title industry must comply with the data safeguarding requirements of the Gramm Leach Bliley Act (GLBA).¹ GLBA places strict requirements on title companies and financial institutions to safeguard "nonpublic personal information". In addition to GLBA, title companies must comply with various state data security and breach notification laws and state insurance department rules like the recent regulation developed by the New York Department of Financial Services. Unlike most federal laws, GLBA does not preempt state law that gives greater privacy protection.

¹ Pub.L. 106-102, 113 Stat. 1338, enacted November 12, 1999.

Several years ago, ALTA developed a set of voluntary industry best practices for members to use as part of their compliance programs. These best practices include guidelines on data security and stronger accounting procedures. This includes things like using secure systems when transmitting a consumer's personal information and ensuring that third parties abide by the title company's data security standards.

While companies are not required to follow the ALTA Best Practices, a significant portion of our membership has adopted them as part of their compliance management program.

Increase in Criminal Activity

Having sound policies and procedures to protect data and money is more important than ever due to the barrage of cyber attacks. Earlier this year, the FBI reported a 480 percent increase in criminals attempting to steal consumer's closing funds.

The growth in the crimes is due in part to their profitability. The average successful bank robber's haul is \$3,816. The average successful wire fraud loss is \$129,427. This is a much better return for a much less expensive and dangerous crime to commit. Overall, these scams have cost Americans \$5.3 billion.

Often, a first step for criminals trying to steal closing funds is deploying a common social engineering technique called phishing. This is a method used by criminals to get you to share your personal information – such as account numbers, Social Security numbers, or your login IDs and passwords. They accomplish this by sending email messages, texts, websites or phone

calls that seem legitimate. Some criminals attempt to get the unsuspecting person to download malicious code. Oftentimes the only goal is to obtain login and password information for your email so that they can use it in another scheme. When these attacks target companies or people that regularly send wire transfer payments, it is called Business E-mail Compromise (BEC) or Email Account Compromise (EAC).²

In a typical scheme targeting homebuyers, the criminal monitors real estate transaction information. In many instances, they obtain access to email accounts, most commonly those used by real estate professionals who are trusted by the consumer. Criminals use this access to find transaction patterns and details to make their fraudulent communications seem legitimate.

Once the criminals gain access to an email account, they will monitor messages to find someone in the process of buying a home. They then use the stolen information to email fraudulent wire transfer instructions disguised to appear as if they came from a professional to the buyer, seller, real estate agent or title company. These emails look legitimate. They often use an actual party's logo, nearly identical email addresses as the supposed sender and use words or phrases gleaned from legitimate emails.

Homebuyers are the most common target. Criminals will monitor email traffic about a transaction to get ahead of common deadlines for the buyer to send the earnest money or down payment. When this occurs, it is not uncommon for the fraud to be discovered weeks later when

² BEC <https://www.ic3.gov/media/2017/170504.aspx>

the buyer shows up to settlement with insufficient funds. This delay in detection also makes it nearly impossible to recover the stolen funds.

In one instance that I am familiar with, a woman in Texas lost her entire life savings to the hands of these sorts of cyber criminals. She had saved nearly \$25,000 and planned to use it as a down payment on a house. Prior to the lender finalizing the Closing Disclosure Form, the woman's email was hacked.

Using information gathered by accessing her email account, a fraudster impersonated the title agency closer, used the closer's name, and instructed the buyer to send the purchase proceeds amount using fraudulent wire instructions. The buyer, believing it was the title agency closer, followed the instructions and wired the funds to the fraudster's account the day before closing. On the day of closing the title agency closer contacted the buyer with the correct amount she needed to purchase the house. Confused, the buyer told the title agency closer that she had already wired the funds according to the closer's earlier instructions. After reviewing the fraudulent wire instructions that the buyer had been sent, the closer contacted the receiving bank to halt the transaction. But it was too late, and the funds had already been sent out. The money was gone. Not only did the home purchase fall through, but the woman lost her life savings.

This form of cybercrime can also wreak irreparable damage on small businesses. In another instance, the email account of an attorney customer of an Illinois based title agency was hacked into. However, the closer at the title agency wasn't aware of the hack. As a result, when the title agency closer was emailed a set of fraudulent disbursement instructions sent by the

fraudster following an initial set of legitimate disbursement instructions sent by the attorney, they simply used what appeared to be the most recent set of instructions sent by their client.

It first became clear that something had gone wrong later that day when the attorney checked with his client as to whether the funds had been received. They had not and so the attorney reached out to the title agency. The title agency immediately reviewed the altered wire instructions and found the owner of the account on those instructions to be different than the sellers. The agency then contacted the bank that wire that received the wire and notified them that it had been fraudulent.

Ultimately the bank on the other end of the transaction was able to freeze the funds, but there were already other wires that had been sent to the same fraudulent account. The title company made the sellers whole by paying them the full sales proceeds of about \$127,000. The company received all but about \$4,000 back, and has used the incident as a valuable training tool for its employees. But had the crime not been detected so early on, this title agency could have suffered a devastating financial loss. Title companies in each of your districts have stories like these.

With the amount of personal data obtained through publicly known data breaches, the risk only increases. In today's environment, criminals can obtain verified email accounts, passwords and security questions on the dark web for as little as \$10.³ Increasingly, criminals do

³ <https://www.bloomberg.com/news/articles/2017-09-15/equifax-hack-your-social-security-and-identity-are-for-sale>

not need to use phishing schemes or other hacking attempts to gain access a real estate professional's email account to perpetuate these crimes.

How the Industry Responded to these Crimes

Title Companies have taken an array of steps to combat this fraud. Some of these steps include using secured email communications, calling homebuyers on a known phone number before sending wire instructions, and asking their banks to match both the recipient's account number a payee information when sending wires. Many of our member companies issue warnings to their customers. They commonly put these warnings on their websites and at the bottom of every email they send.

This is not a problem that we as an industry can fix on our own. What is so frustrating is that there is no amount of money we can spend to protect our consumers from being targeted by these criminals. The only thing that will help is to increase awareness so that our customers can help protect themselves.

At ALTA, this has been our guiding principle this year. In April, we issued a consumer alert outlining five tips that people can use to protect against wire fraud:

1. **Call, don't email:** Confirm all wiring instructions by phone before transferring funds.
Use the phone number from the title company's website or a business card.
2. **Be suspicious:** It's not common for title companies to change wiring instructions and payment information.

3. **Confirm it all:** Ask your bank to confirm not just the account number but also the name on the account before sending a wire.
4. **Verify immediately:** You should call the title company or real estate agent to validate that the funds were received. Detecting that you sent the money to the wrong account within 24 hours gives you the best chance of recovering your money.
5. **Forward, don't reply:** When responding to an email, hit forward instead of reply and then start typing in the person's email address. Criminals use email address that are very similar to the real one for a company. By typing in email addresses you will make it easier to discover if a fraudster is after you.

We then converted that alert into a 2-minute video that title companies, real estate agents and lenders can use to help educate consumers about how they protect their money.⁴ We also developed an info-graphic that members can use to inform homebuyers about the wire fraud scams and what to do if they've been targeted by a scam.

Our members know the key to keeping these crimes from happening in their community is awareness, and they know they cannot do it alone. This needs to be a coordinated awareness effort across the industry between all players including real estate agents, policy makers, consumer groups, title insurance companies, title and settlement agents, real estate attorneys and customers themselves.

In January of this year, I along with the ALTA Board of Governors met with Consumer Financial Protection Bureau Director Richard Cordray. In that meeting, we provided examples of

⁴ Video (linked)

these crimes and asked for the CFPB's help in increasing awareness. They were not aware of this crime and asked for more information, which our members were happy to provide. We followed up with a letter to the Bureau in April. We said, "Despite efforts by the title industry and others to educate consumers about the risk, homebuyers continue to be targeted. If we are going to protect consumers from these schemes during the upcoming home buying season we will need your help." We encouraged the Bureau to work with its fellow financial regulators and law enforcement officials to prevent these criminals from utilizing our country's financial system.

In July, the CFPB published a warning to help alert consumers about wire fraud schemes.⁵ Other regulators have also issued warnings including the Missouri Department of Insurance (DOI), the Colorado Division of Real Estate at the Department of Regulatory Agencies, the Federal Trade Commission and the Financial Crimes Enforcement Network (FinCEN).

While this is a step in the right direction, this alone will not solve this problem. We all need to use consumer alerts to help educate our buyers, sellers and real estate partners about the risks. We need to carry an urgency about this problem. Consumers need to not just be aware of the danger, but empowered to help protect themselves.

Additional Practices to Prevent Fraud

Along with increasing awareness for homebuyers, we are working with our industry partners to make simple process changes to help consumers.

⁵ <https://www.consumerfinance.gov/about-us/blog/buying-home-watch-out-mortgage-closing-scams/>

Probably the single biggest preventative measure that real estate and banking professionals can take is to encourage consumers to call the title company or real estate agent to verify wire instructions before transmitting funds. We encourage regulators to work with banks to include this simple practice into their training in working with customers that are sending wires for real estate purchases.

Another banking practice that would help reduce the risk is payee matching. We encourage financial institutions to match not only the account number of the recipient but also the payee's name. Oftentimes the fraudulent instructions will say the transfer is to be sent to the title company's trust account but instead it goes to the criminal's personal account. Just matching the account number on the request with an account number at the beneficiary bank will not catch this. Some banks have voluntarily added additional capabilities to match the payee's names, and it is proving useful in catching these schemes.

Conclusion

Consumer losses due to a data breach (even a massive one like Equifax), pales in comparison to the loss of their down payment or earnest money. We believe policy makers should focus on two key areas to stop these crimes.

First, we need to increase public awareness of these schemes. In an advisory last year, the Financial Crimes Enforcement Network (FinCEN) stated that due to the irrevocable nature of these transfers, the best first line of defense is to prevent Americans from falling victim to these scams.

Second, a simple change in practices can be the single biggest deterrent to wire fraud. We encourage financial institutions to match not only the account number of the beneficiary but also the payee's name.

Lastly, policymakers should consider ways to better use both suspicious activity reports and IC3 data to better detect accounts used by these criminals and their mules. We need to provide financial institutions with as much information as possible to uncover these networks. Even if more information does not lead to prosecutions of these criminals, it can help banks decide to place holds on the account preventing the criminal or the mule from withdrawing funds while they conduct a more thorough investigation.

I appreciate the opportunity to discuss one of the largest threats to consumers, title companies and the U.S. real estate system. ALTA is eager to serve as a resource to this Subcommittee, and I am happy to answer any questions.

**Testimony of Edmund Mierzwinski,
U.S. PIRG Consumer Program Director
Hearing on “Data Security: Vulnerabilities and Opportunities for Improvement”**

**Before the House Committee on Financial Services,
Subcommittee on
Financial Institutions and Consumer Credit**

Honorable Blaine Luetkemeyer, Chair

1 November 2017

**Testimony of Edmund Mierzwinski, U.S. PIRG Consumer Program Director Before the Committee on
Financial Services, Subcommittee on Financial Institutions and Consumer Credit**

Chairman Luetkemeyer, Representative Lacy Clay, members of the committee, I appreciate the opportunity to testify before you on the important matter of data security and cyber threats. Since 1989, I have worked on data privacy issues, among other financial system and consumer protection issues, for the U.S. Public Interest Research Group. The state PIRGs are non-profit, non-partisan public interest advocacy organizations that take on powerful interests on behalf of their members.

Summary:

As stated in the committee's staff memo: "Congress must thoroughly examine data security vulnerabilities and the shortcomings of the existing federal and state regulatory regimes to identify any gaps in data security regulation and highlight opportunities for reform."

I construe data security and the issues it raises broadly in this testimony to include an examination not only of data security and proper data breach response. I also review the history of how public policy decisions trending against the concept of consumer privacy have encouraged and promoted greater collection, sale and sharing of consumer information – without concomitant consumer control, without adequate regulatory requirements for data security, and certainly without market incentives for firms to protect the consumer financial DNA they collect and then sell.

I urge the Congress, at a minimum, to enact free credit freeze legislation. I caution the Congress, however, not to move forward on any breach or data security legislation that would preempt strong state privacy leadership or would endorse closed or non-technology neutral standards. Federal law should never become a ceiling of protection, it should always serve as a minimal floor that allows state experimentation. Further, federal law should not endorse specific solutions that limit innovation.

I. Introduction:

While I note that thorough questioning by members at the previous committee hearing featuring Richard Smith, the *ex-CEO* of Equifax, helped to confirm numerous problems with Equifax security and its response to the breach, it is telling that Equifax and its competitor Big 3 consumer credit reporting agencies Experian and Transunion all chose to ignore Congressional requests to send their current CEOs to that continuation hearing. What do they have to hide?

The authoritative Privacy Rights Clearinghouse has estimated that at least 1,073,490,127 records have been breached in a total of at least 7,730 data breach occurrences made public since 2005.¹ The latest exploit, against Equifax, a major consumer credit reporting agency (colloquially, a credit bureau), not only affected at least 145.5 million consumers, but compromised perhaps the richest trove of personal information I have seen in my over

¹ See Data Breach page at Privacy Rights Clearinghouse, last visited 30 October 2017, <https://www.privacyrights.org/>.
Testimony of Edmund Mierzwinski, U.S. PIRG, 1 Nov 2017

years of privacy and data security research.² While Yahoo³ now says all 3 billion of its user accounts may have been breached in 2013, much of the information taken could only be used for “phishing” emails or “social engineering” phone calls designed to use a little information to try to gain a lot more. While the Target⁴ and other retail breaches resulted in the theft of millions of credit and debit card numbers, those numbers can only be used in the short-term for “existing account fraud” before banks change the numbers.

A. The Loss By Equifax Of The Bits And Pieces Of Your Financial DNA Is Worse Than A Card Breach:

Dates of birth and Social Security Numbers do not change. They do not have a shelf life and can be used for more serious identity theft such as hard-to-deal-with new account fraud, tax refund fraud, and theft of medical services. To me, the Equifax breach is rivaled only by the loss of similar information for 22 million employees, applicants and even friends providing character references for those applicants by the U.S. Office of Personnel Management (OPM)⁵ in 2015.

Unlike credit card numbers, your Social Security Number and Date of Birth don’t change and may even grow more valuable over time, like gold in a bank vault. Much worse, they are the keys to “new account identity theft,” which can only be prevented by a credit report freeze, as discussed in detail at the last hearing.⁶ While Equifax and other consumer credit reporting companies are required by the Fair Credit Reporting Act (FCRA) to make it hard for imposters to obtain another’s credit report (how many security questions did you answer to obtain your own report?); identity thieves don’t want your credit report. Instead, they use your SSN and DOB to apply for credit in your name; so that the bank or other creditor, which is a trusted third party (and likely answers no security questions) with easy access to the credit reporting company, obtains your credit report and/or credit score and then wrongly issues credit to the thief. In the U.S., such new account identity theft is fueled both by the high demand for “instant credit” and by that critical flaw in our credit granting system, where SSNs serve as both a matching identifier in databases and as an authenticator of a consumer applicant.⁷

² Equifax’s primary and best-known business is as one of three (Experian and Transunion are the others) national “Consumer Reporting Agencies” (colloquially “credit bureaus”) that do their consumer reporting business under the Fair Credit Reporting Act (FCRA) but also engage in a wide variety of lightly to unregulated direct marketing as “data brokers.”

³ Lily Hay-Newman, “Yahoo’s 2013 Email Hack Actually Compromised Three Billion Accounts,” 3 October 2013, <https://www.wired.com/story/yahoo-breach-three-billion-accounts/>

⁴ The Target breach reportedly exposed 40 million credit and debit card numbers, as well as the customer account records – including phone numbers and emails – of millions more consumers. See Eric Dezenhall, “A Look Back at the Target Breach,” 6 June 2015, https://www.huffingtonpost.com/eric-dezenhall/a-look-back-at-the-target_b_7000816.html

⁵ Brendan I. Koerner, “Inside the Cyberattack That Shocked the US Government,” 23 October 2017, <https://www.wired.com/2016/10/inside-cyberattack-shocked-us-government/>

⁶ See testimony of Mike Litt, U.S. PIRG before the committee, 25 October 2017, available at <https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-mlitt-20171025.pdf>

⁷ See “Security In Numbers: SSNs and Identity theft,” an FTC report, which discusses the problems of using Social Security Numbers to authenticate people even though they are not secret, but ubiquitous and widely available to thieves, December 2008, available at <https://www.ftc.gov/sites/default/files/documents/reports/security-numbers-social-security-numbers-and-identity-theft-federal-trade-commission-report/p075414ssnreport.pdf>

Testimony of Edmund Mierzwinski, U.S. PIRG, 1 Nov 2017

**B. And Even Worse, The Equifax Breach Was By A Data Broker: A Firm With Only One Job—
Buying And Selling Consumer Information:**

Equifax should do better at protecting data: it is a data broker, not a corner store, department store, health care provider or government agency. Incredibly, this is not the first security problem Equifax has faced recently.⁸

Equifax should have had a deeper moat and thicker castle walls, with more cross-bow archers, more trebuchets and more cauldrons of boiling oil on the watchtowers to defend your data than a merchant or even a government agency. It did not.

Regarding the committee's specific Equifax hearings, I associate my remarks completely with all recommendations of my consumer advocacy colleagues and state attorneys general experts at the committee's "Continuation of the Equifax Hearing" requested by Ranking Member Maxine Waters (CA), last week.⁹ Of course, I also believe that the minimum action Congress should take would be to extend free credit freezes at all 3 national consumer reporting agencies to all consumers at all times. The committee should also ensure one-stop shopping for credit freezes, as is already the law for fraud alerts. You should need to contact only one credit bureau to gain protection at all three.

**C. The Paradox of Equifax: Highly Regulated When It Sells Credit Reports Yet Not Really Regulated
When It Sells Other Products as a Data Broker**

The Paradox of Consumer Credit Reports vs. Other Data Products: The Equifax breach extensively reviewed in two previous full committee hearings demonstrates several paradoxes of our data use, privacy and data security laws and regulations. While the security of the *consumer credit reports* sold by Equifax in its role as a Consumer Reporting Agency (CRA) is strictly regulated by the Fair Credit Reporting Act (FCRA),¹⁰ the security of the *Social Security Numbers and Dates of Birth and other personally-identifiable-information (PII)* lost in the breach is regulated only under the limited data security requirements of Title V of the Gramm-Leach-Bliley Act (15 U.S.C. 6801 et seq.).¹¹ In addition, other (non-credit report) consumer profiles sold by Equifax and its hundreds, or thousands, of competitors in the *data broker* business are hardly regulated at all.

⁸ Thomas Fox-Brewster, "A Brief History of Equifax Security Fails," 8 September 2017, Forbes.
<https://www.forbes.com/sites/thomasbrewster/2017/09/08/equifax-data-breach-history/#192afb0a677c>

⁹ Continuation of Hearing entitled "Examining the Equifax Data Breach,"

25 October 2017, witness statements available at

<https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=402472>

¹⁰ 15 U.S.C. 1681 et seq.

¹¹ The prudential regulator rules implementing Title V of GLBA generally only require that a breach notice plan be "considered." See bank regulators' joint "Interagency Guidelines Establishing Information Security Standards" are available at: <https://www.fdic.gov/regulations/laws/rules/2000-8660.html> The FTC Safeguards Rule applicable to national consumer credit reporting agencies including Equifax, which is silent on breach notification, is available here: https://www.ftc.gov/sites/default/files/documents/federal_register_notices/standards-safeguarding-customer-information-16-cfr-part-314/020523standardsforsafeguardingcustomerinformation.pdf The FTC is currently adding elements of a breach notification plan to its 2002 final rule above. All documents related to Title V are archived by the FTC here: <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule>

Testimony of Edmund Mierzwinski, U.S. PIRG, 1 Nov 2017

The Federal Trade Commission has recognized this. In two major reports in the last 5 years, it has called for greater authority to regulate the collection, sharing and sale of consumer information outside the limited walls of the FCRA, which primarily applies only to reports used in the determination of a consumer's eligibility for credit, insurance or employment. From the FTC's landmark report recommending Congress give it more authority over data brokers:¹²

"Data brokers obtain and share vast amounts of consumer information, typically behind the scenes, without consumer knowledge. Data brokers sell this information for marketing campaigns and fraud prevention, among other purposes. Although consumers benefit from data broker practices which, for example, help enable consumers to find and enjoy the products and services they prefer, data broker practices also raise privacy concerns. [...] Data brokers combine and analyze data about consumers to make inferences about them, including potentially sensitive inferences such as those related to ethnicity, income, religion, political leanings, age, and health conditions. Potentially sensitive categories from the study are "Urban Scramble" and "Mobile Mixers," both of which include a high concentration of Latinos and African-Americans with low incomes. The category "Rural Everlasting" includes single men and women over age 66 with "low educational attainment and low net worths." Other potentially sensitive categories include health-related topics or conditions, such as pregnancy, diabetes, and high cholesterol."

When the Big 3 credit bureaus are in their alternate guise as nearly unregulated data brokers, they sell numerous consumer profiles to businesses. Consumers have no rights to know about these files, to examine these files, to correct these files or to limit their use. Congress should consider the FTC's proposals.

- The data broker Experian:¹³ "New markets targeted. Response rates improved. Revenue increased. These are the results we at Experian, as the industry leader, help you achieve with our business services."
- The data broker Equifax:¹⁴ "The power behind our solutions—and your acquisition programs—is the superior quality of our data."
- The data broker Transunion:¹⁵ "TransUnion offers more complete and multidimensional information for informed decisions that create opportunities for your business."

Paradox: the FCRA is One of our Strongest Privacy Laws: Despite the abysmal failure over the years of firms regulated under the FCRA to maintain the accuracy of consumer credit reports, or to adequately respond to consumers who dispute the inaccuracies that harm their financial or employment opportunities,¹⁶ it remains that the 1970 FCRA's framework is fundamentally based on the Code of Fair Information Practices (FIPs), developed by a committee of the HEW Advisory Committee on Automated Data Systems in 1972, which was codified in the

¹² FTC News Release, "Agency Report Shows Data Brokers Collect and Store Billions of Data Elements Covering Nearly Every U.S. Consumer," 27 May 2014, <https://www.ftc.gov/news-events/press-releases/2014/05/ftc-recommends-congress-require-data-broker-industry-be-more>

¹³ <http://www.experian.com/business-services/business-services.html>

¹⁴ <http://www.equifax.com/business/acquire-more-customers>

¹⁵ <https://www.transunion.com/business>

¹⁶ "...the credit reporting agencies have grown up in a culture of impunity, arrogance, and exploitation. For decades, they have abused consumers, cut corners in personnel and systems, and failed to invest in measures that would promote accuracy or handle disputes properly." See page 3, testimony of Chi Chi Wu, National Consumer Law Center, before the committee on 25 October 2017, available at <https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-ccwu-20171025.pdf>

Testimony of Edmund Mierzwinski, U.S. PIRG, 1 Nov 2017

1974 U.S. Privacy Act and governs information use by federal agencies.¹⁷ The Privacy Rights Clearinghouse notes:

"In contrast to other industrialized countries throughout the world, the U.S. has not codified the Fair Information Principles into an omnibus privacy law at the federal level. Instead, the Principles have formed the basis of many individual laws in the U.S., at the both federal and state levels -- called the "sectoral approach." Examples are the Fair Credit Reporting Act, the Right to Financial Privacy Act, the Electronic Communications Privacy Act, and the Video Privacy Protection Act.¹⁸"

The FIPs are nevertheless embodied in the FCRA: The FCRA limits the use of consumer credit reports only to firms with certain permissible purposes (generally, determinations of a consumer's eligibility for credit, insurance and employment), it requires credit bureaus (data collectors) to meet certain accuracy standards and it allows consumers to review their files, dispute and demand corrections of mistakes and to control the secondary use of their files by opting out of marketing uses of their reports.

Nevertheless, the U.S. sectoral-only privacy laws should be contrasted with the new European **General Data Protection Regulation (GDPR)**. It provides over-arching privacy rights to European citizens over corporate usage of their information, including rights to control the use of their information and to seek redress (and compensation) against the infringing company. Importantly, the GDPR, when it goes into final effect next year, trumps the existing Privacy Shield¹⁹ applicable to U.S. firms doing business in Europe and provides a roadmap for U.S. companies to improve their treatment of U.S. consumers.²⁰

In particular, since SIFMA member firms will be subject to the GDPR, it seems that they can import those protections to small investors in the U.S., rather than seek, as they may today, to weaken applicability of existing state data security and identity theft laws.

The Paradox of Identity Theft as a Business Opportunity: The big credit bureaus have responded to the scourge of identity theft driven by instant credit, sloppy credit report-granting practices, and of course, data breaches, not by improving their own security and compliance but by seizing new business opportunities:

Consumers scared of either fraud and identity theft or low credit scores are urged to buy their subscription credit monitoring services, for as much as \$10-20/month. The GAO has determined that such "services offer some benefits but are limited in preventing fraud."²¹ Estimates are that consumers spend at least \$3 billion/year on credit monitoring services.²²

¹⁷ "U.S. Dep't. of Health, Education and Welfare, Secretary's Advisory Committee on Automated Personal Data Systems, Records, computers, and the Rights of Citizens viii (1973)", https://cpic.org/privacy/consumer/code_fair_info.html

¹⁸ Privacy Rights Clearinghouse, "A Review of The Fair Information Principles: The Foundation Of Privacy Public Policy," 1 October 1997, <https://www.privacyrights.org/blog/review-fair-information-principles-foundation-privacy-public-policy>

¹⁹ For information on the Privacy Shield, see <https://www.ftc.gov/tips-advice/business-center/privacy-and-security/privacy-shield>

²⁰ The GDPR is explained here https://en.wikipedia.org/wiki/General_Data_Protection_Regulation

²¹ U.S. General Accounting Office, March 2017: "Identity Theft Services: Services Offer Some Benefits but Are Limited in Preventing Fraud," <http://www.gao.gov/assets/690/683842.pdf>

²² Steve Weisman, "Is Identity Theft Protection Worth It?", 22 April 2017, USA Today, <https://www.usatoday.com/story/money/columnist/2017/04/22/identity-theft-protection-worth/100554362/>

Testimony of Edmund Mierzewski, U.S. PIRG, 1 Nov 2017

Despite that the bureaus have failed to either protect credit reports or maintain the “maximum possible accuracy” required by law, they have also monetized a lucrative business-to-consumer (B2C) channel for over 20 years to market their over-priced, under-performing credit monitoring products.²³

And of course, the big credit bureaus and others have also leapt into the business of B2B identity validation and verification, largely in response to their own, and others’, failure to maintain the security of information.

The Paradox of Businesses as Customers and Consumers as Products: Despite nearly 50 years of FCRA requirements to handle consumer disputes and over 20 years of aggressive-direct-to-consumer advertising of pricy subscription-based credit monitoring products, its ex-CEO repeatedly apologized to Congress that, as a business-to-business company, it had no idea how many consumers would call or email. How is this possible? Well, it turns out consumers are not looked at by Equifax as customers.

This absurd disconnect is because of a market failure in credit reporting; we are not their customers, we are their product. The consumer credit reporting market is dominated by the Big 3 gatekeepers to financial and employment opportunity. Yet, you cannot choose a credit bureau. When you are mad at your bank’s fees or policies, you can vote with your feet and find a new bank. You’re stuck with the credit bureaus. Richard Cordray, director of the Consumer Financial Protection Bureau, often calls credit reporting one of several “dead-end markets” in need of stricter regulation to counter that market failure.²⁴

The Big 3 bureaus (Equifax, Experian and Transunion) were fined an inadequate total of \$2.5 million by the Federal Trade Commission (in 2000) for failing to have enough employees to answer the phones to handle their complaints.²⁵

Nevertheless, we are encouraged by the recent efforts by the Consumer Bureau to achieve changes to the Big 3’s operations through supervision.²⁶

Consumers Have Little Control of their Information: The 1999 Gramm-Leach-Bliley Financial Modernization Act was largely enacted to allow mergers of commercial banks, investment banks, securities firms and insurance companies. However, due to privacy complaints at the time about a number of large banks, including U.S. Bank,

²³ On 7 September 2017, the date that the Equifax breach was announced to the public, the committee held a hearing on a discussion draft from Mr. Royce, a bill which we oppose. The bill would exempt credit bureau marketing and education programs from the Credit Repair Organizations Act, and exempt the bureaus, and others that might seek the same license, from strong consumer protection laws. The discussion draft is available at https://financialservices.house.gov/uploadedfiles/bills-115_royce020_pih.pdf. We concur with Chi Chi Wu’s testimony against both the Royce bill and against a bill from Mr. Loudermilk also discussed that day. HR2359, the so-called FCRA Liability Harmonization Act, would eliminate punitive damages and cap other damages in actions brought under the FCRA. Testimony of Chi Chi Wu, National Consumer Law Center is available at <https://financialservices.house.gov/uploadedfiles/hrg-115-ba15-wstate-ccwu-20170907.pdf>.

²⁴ Richard Cordray, “Prepared Remarks of CFPB Director Richard Cordray at the National Association of Attorneys General,” 23 February 2015, <https://www.consumerfinance.gov/about-us/newsroom/prepared-remarks-of-cfpb-director-richard-cordray-at-the-national-association-of-attorneys-general-2/>.

²⁵ Press release, “Nation’s Big Three Consumer Reporting Agencies Agree To Pay \$2.5 Million To Settle FTC Charges of Violating Fair Credit Reporting Act,” 13 January 2000, available at <https://www.ftc.gov/news-events/press-releases/2000/01/nations-big-three-consumer-reporting-agencies-agree-pay-25>.

²⁶ Consumer Financial Protection Bureau, “Supervisory Highlights: Consumer Reporting, Special Edition,” March 2017, Issue 14, Winter 2017, available at http://files.consumerfinance.gov/f/documents/201703_cfpb_Supervisory-Highlights-Consumer-Reporting-Special-Edition.pdf.

Testimony of Edmund Mierzwinski, U.S. PIRG, 1 Nov 2017

which was sued by the State of Minnesota for sharing customer records with a third-party telemarketer that then preyed on its customers.²⁷ the law did include a modest privacy and data security provision, Title V, that gave consumers the ability to opt-out of sharing of their personal information only with non-affiliated, non-financial firms (but explicitly allowed sharing with affiliates or other financial firms, regardless of a consumer's wishes).²⁸ A wide variety of organizations, ranging from the ACLU to consumer groups to Phyllis Schlafly's Eagle Forum, supported more comprehensive privacy protection provisions proposed by a broadly bi-partisan group led by then-Rep. Ed Markey (D-MA) and Rep. Joe Barton (R-TX).²⁹

The final law also required banks and certain non-banks, including consumer credit reporting firms, to comply with its data security provisions.³⁰

Although the 2010 Dodd-Frank Act enacted in the wake of the 2008 financial collapse transferred authority to regulate credit reporting under FCRA to the tough new Consumer Financial Protection Bureau, its Section 1093 retained Title V data security provisions for non-banks under the weaker FTC. Unlike CFPB, that agency cannot supervise the activities of firms on a day-to-day basis, nor can it impose civil money penalties for a first violation.

The Congress Needs To Allow Consumers To Hold Firms More Accountable: In the immediate circumstance, the best way to give consumers protection against data breaches is to hold firms that lose our information accountable, including through their wallets. Threats to consumers can include fraud on existing accounts, new account identity theft, medical identity theft, tax refund identity theft and imposters committing crimes using your identity. Measurable harms from these misuses are obvious, but any measure of harms must also include the cost and time spent cleaning these problems up, additional problems caused by an empty checking account or a missing tax refund and being denied or paying more for credit or insurance or rejected for jobs due to the digital carnage caused by the thief. Consumers also face very real emotional stress and even trauma from financial distress. Breach harms also include the threat of physical harm to previous domestic violence victims.³¹

²⁷ "Defendants US Bank National Association ND and its parent holding company, US Bancorp, have sold their customers' private, confidential information to MemberWorks, Inc., a telemarketing company, for \$4 million dollars plus commissions of 22 percent of net revenue on sales made by MemberWorks." Complaint filed by the State of Minnesota against U.S. Bank, 9 June 1999, available on Internet Archive, last visited 30 October 2017, https://web.archive.org/web/20010423055717/http://www.ag.state.mn.us:80/consumer/privacy/pr/pr_usbank_06091999.html

²⁸ The 1999 GLBA required annual privacy notices of financial institution information sharing practices and of the limited right to opt-out it provided. Industry organizations have relentlessly sought to eliminate the annual notice provisions. A transportation bill known as the FAST Act codified a narrowing of the requirement as a rider in 2015, as explained by the Consumer Financial Protection Bureau, <https://www.federalregister.gov/documents/2016/07/11/2016-16132/annual-privacy-notice-requirement-under-the-gramm-leach-bliley-act-regulation-p> HR 2396. We also oppose "The Privacy Notification Technical Clarification Act," to further narrow consumer rights to notice about privacy practices, was approved by this committee in a markup held on 11-12 October 2017, <https://financialservices.house.gov/calendar/eventsingle.aspx?EventID=402416>

²⁹ The variety of groups that worked together for stronger privacy provisions is listed in this letter of 9 May 2000 to prudential regulators urging faster compliance of stronger rules, available on Internet Archive, last visited 30 October 2017, <https://web.archive.org/web/20010425154255/http://www.pirg.org:80/consumer/glbdelay.htm>

³⁰ The Federal Trade Commission's 2002 Safeguards Rule implements the law for non-bank "financial institutions, including the consumer reporting agencies and is available at <https://www.ftc.gov/enforcement/rules/rulemaking-regulatory-reform-proceedings/safeguards-rule>

³¹ See Page 10, Testimony of Laura Moy, Deputy Director, Center on Privacy and Technology, Georgetown University Law Center, 25 October 2017, available at: <https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-lmoy-20171025.pdf>

Testimony of Edmund Mierzwinski, U.S. PIRG, 1 Nov 2017

II. Detailed Recommendations:

1) Congress should not enact any federal breach law that preempts stronger state breach notification laws or related protections:

In 2003, when Congress, in the FACT Act, amended the Fair Credit Reporting Act, it specifically did not preempt the right of the states to enact stronger data security and identity theft protections. We argued that since Congress hadn't solved all the problems, it shouldn't prevent the states from doing so.³²

From 2004-today, nearly every state enacted security breach notification laws and enacted credit, or security, freeze laws. Many of these laws were based on the CLEAN Credit and Identity Theft Protection Model State Law³³ developed by Consumers Union and U.S. PIRG.

Congress should not preempt stronger state breach notification laws. **California** and **Texas**, for example, have very strong notification laws based on an *acquisition* standard. Information lost is presumed to be acquired, therefore requiring notice to breach victims. Industry actors would prefer use of a *harm trigger* before notice is required.

There are numerous problems with a harm trigger, which is a feature of some state laws and most proposed federal laws. The first is that the breached entity, which has already demonstrated extreme sloppiness with the personal information of its customers, gets to decide whether to inform them so that they can protect themselves.

The second problem is that industry groups would like any preemptive federal bill to define privacy harms very narrowly; their preferred bills would limit harms to direct financial harm due to identity theft.

Yet harms also include the cost and time spent cleaning these problems up, additional problems caused by an empty checking account or a missing tax refund and being denied or paying more for credit or insurance or rejected for jobs due to the digital carnage caused by the thief. Further, consumers face very real additional problems including the stigma of being branded a deadbeat and facing the emotional costs and worry that brings.

Only an acquisition standard will serve to force data collectors to protect the financial information of their trusted customers or accountholders well enough to avoid the costs, including to reputation, of a breach. Only if an entity's reputation is at risk will it do its best job to protect your reputation.

Further, as Laura Moy extensively pointed out at this committee's hearing last week, potential harms to consumers from misuse of information go well beyond financial identity theft.

"In addition, trigger standards narrowly focused on financial harm ignore the many non-financial harms that can result from a data breach. For example, an individual could suffer harm to dignity if he stored embarrassing photos in the cloud and those photos were compromised. If an individual's personal email were compromised and private emails made public, she could suffer harm to her reputation. And in some

³² For a detailed discussion of how the FACT Act left the states room to innovate, see Gail Hillebrand, "After the FACT Act: What States Can Still Do to Prevent Identity Theft," 13 January 2004, available at <http://consumersunion.org/research/after-the-fact-act-what-states-can-still-do-to-prevent-identity-theft/>

³³ U.S. PIRG and Consumers Union, "The Clean Credit and Identity Theft Protection Act: Model State Laws - A Project of the State Public Interest Research Groups and Consumers Union of U.S., Inc." Version of November 2005, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=846505

Testimony of Edmund Mierzwinski, U.S. PIRG, 1 Nov 2017

circumstances, breach could even lead to physical harm. For example, the fact that a domestic violence victim had called a support hotline or attorney, if it fell into the wrong hands, could endanger her life.”³⁴

Ms. Moy’s testimony is a magisterial analysis of the ways many broader state law protections would be eliminated by a narrow, preemptive federal bill. Bad outcomes she describes range from elimination of broad definitions of harms requiring notice and elimination of growing types of information protected by state laws (including **California, Florida, and Texas** laws requiring protection of physical and mental health records, medical history, and insurance information as well as elimination of a variety of state laws protecting online credentials, GPS data and biometric data). Ms. Moy also correctly urges the committee to leave the states room to respond to new, unknown threats.³⁵ Again, this is what the Congress did in the 2003 Fair and Accurate Transactions Act amendments to the FCRA, when it left the states free to respond to identity theft.

At that same hearing, **New York** Assistant Attorney General Kathleen McGee also notes that state notification laws have been expanded to include account credentials, biometric data and other protections. She also notes that nearly every state also holds firms accountable based on their consumer protection laws, which would also be preempted by many federal proposals.³⁶

Other state attorneys general concur. As a news release accompanying **Illinois** Attorney General Lisa Madigan’s recent testimony³⁷ to the U.S. Senate explained:

“The Attorney General also testified that a federal data breach law must cover a broad range of sensitive data – not just social security numbers or stolen credit card numbers but also: online login credentials, medical information shared on the internet that is outside the scope of current privacy regulations, biometric data, and geolocation data. Companies must be required to report any data breach involving this type of personal information, Madigan said. Equally as important as Congress considers a federal data breach notification law, Madigan said, is the ability for state regulators to continue investigating data breaches at the state level. Federal legislation must not preempt the states’ ability to respond and act when data breaches affect residents in their states. Any preemption by Congress must only provide a “floor” for reporting requirements and preserve a state’s ability to use its consumer protection laws to investigate data security practices and enforce federal law.”³⁸

³⁴ See section 3, especially, of testimony of Laura Moy, Georgetown University Law Center’s Center on Privacy and Technology, before this committee on 25 October 2017, available at <https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-lmoy-20171025.pdf>

³⁵ Testimony of Laura Moy, Georgetown University Law Center’s Center on Privacy and Technology, before this committee on 25 October 2017, available at <https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-lmoy-20171025.pdf>

³⁶ Testimony of Kathleen McGee, Assistant Attorney General, Office of the New York Attorney General, at a hearing before this committee on 25 October 2017, available at <https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-kmcgee-20171025.pdf>

³⁷ “Getting it Right on Data Breach and Notification Legislation in the 114th Congress,” A Hearing of the U.S. Senate Committee on Commerce, 5 February 2015, available at <http://1.usa.gov/1tGf5m>

³⁸ Excerpt from news release: “Madigan: Federal Data Breach Law Should Not Weaken States’ Consumer Protections”, 5 February 2015, available at http://www.illinoisattorneygeneral.gov/pressroom/2015_02/20150205.html

Testimony of Edmund Mierzwinski, U.S. PIRG, 1 Nov 2017

General Madigan's office is also actively involved in the multi-state Equifax investigation, is calling for Equifax to pay for credit freezes for all Illinois residents and is supporting state legislation to provide free credit freezes.³⁹

2) Congress Should Not Enact a Narrow, Preemptive Breach Law That Also Includes a Trojan Horse Provision to Preempt Broader State Data Security and Privacy Laws:

The other problem with enacting a preemptive federal breach notification law is that industry lobbyists will seek language that not only preempts state breach notification laws but also prevent states from enacting any future data security or privacy laws. This is the Trojan Horse problem. A small federal gain should not result in a big rollback of state authority.

As one example of a Trojan Horse provision I call your attention to a bill approved by this committee in the last Congress. HR 2205,⁴⁰ the Data Security Act of 2015 (Neugebauer), included sweeping preemption language that is unacceptable to consumer and privacy groups and likely also to most state attorneys general. While I note that this bill has numerous other objectionable provisions, which I am happy to discuss, its sweeping preemption language is illustrative of long-sought industry goals to take states off the board:

SEC. 6. RELATION TO STATE LAW.

No requirement or prohibition may be imposed under the laws, rules, or regulations of any State, the District of Columbia, or any territory of the United States with respect to the responsibilities of any person to--

- (1) protect the security of information relating to consumers that is maintained, communicated, or otherwise handled by, or on behalf of, the person;
- (2) safeguard information relating to consumers from--
 - (A) unauthorized access; and
 - (B) unauthorized acquisition;
- (3) investigate or provide notice of the unauthorized acquisition of, or access to, information relating to consumers, or the potential misuse of the information, for fraudulent, illegal, or other purposes;
- (4) mitigate any potential or actual loss or harm resulting from the unauthorized acquisition of, or access to, information relating to consumers.

Other bills before the Congress have included similar, if not even more sweeping, dismissals of our federal system. Such broad preemption will prevent states from acting as innovators of public policy or as first responders to emerging privacy threats. Congress should not preempt the states but instead always enact a floor of protection. In fact, Congress should think twice about whether a federal breach law that is weaker than the best state laws is needed at all. Congress should maintain co-authority of state Attorney General and other state and local enforcers; Congress should also retain state private rights of action, especially if it declines to create any federal private rights of action.

³⁹ News Release, 12 September 2017, available at http://www.illinoisattorneygeneral.gov/pressroom/2017_09/20170912.html

⁴⁰ HR 2205 is available at <https://www.congress.gov/bills/114/congress-house-bill/2205/>

Testimony of Edmund Mierzwinski, U.S. PIRG, 1 Nov 2017

The testimony of Sara Cable, a **Massachusetts** Assistant Attorney General, before this committee, makes several points about the importance of state action abundantly clear:

“The Equifax breach may bring into consideration whether a national data breach notice and data security standard is warranted. As noted, Massachusetts has among the strongest data security and breach laws in the country. My Office has serious concerns to the extent any federal standard seeks to set weaker standards than those that currently exist for Massachusetts consumers and that would preempt existing or future state law in this field. States are active, agile, and experienced enforcers of their consumers’ data security and privacy, and need to continue to innovate as new risks emerge.”⁴¹

Ms. Cable’s testimony also notes Massachusetts Attorney General Maura Healey’s strong support for free credit freeze legislation to be enacted by the state.

To the extent any national standard is considered by the committee, it must contain strong, minimum data security standards that do not erode existing state protections.

3) Congress Should Enact A Free Credit Freeze For All Law and Implement One-Stop Shopping for Freezes

Of course, I also believe that the minimum action Congress should take would be to extend free credit freezes at all 3 national consumer reporting agencies to all consumers at all times. The need for a free credit freeze to prevent identity theft was discussed in detail before the committee hearing last week by my colleague Mike Litt.⁴² The committee should also ensure one-stop shopping for credit freezes, as is already the law for fraud alerts. You should need to contact only one credit bureau to gain protection at all three.

Mr. Litt’s testimony also highlighted numerous other issues pertaining to how Equifax, Trans Union and Experian offer their own inferior packages of “locks” and other products that may force consumers to accept unfair terms and conditions with diminished rights and protections. Congress should also provide breach victims with an additional free credit from each national bureau.

4) The Congress Should Transfer Authority Over Gramm-Leach-Bliley Title V to the Consumer Bureau

We are encouraged that at the first Equifax hearing, that the full committee chairman, Mr. Hensarling, supported a review of the Gramm-Leach-Bliley framework, when he said “We must thoroughly examine if our agencies and statutes like Gramm, Leach, Bliley; the Fair Credit Reporting Act; and UDAAP [Unfair, Deceptive, Abusive Acts and Practices] are up to the job”.⁴³

We support, as did the National Consumer Law Center at last week’s hearing, transferring Gramm-Leach-Bliley Title V responsibilities to the CFPB from the Federal Trade Commission. The FTC cannot impose civil penalties

⁴¹ Testimony of Sara Cable, Assistant Attorney General, Office of the Massachusetts Attorney General, before this committee, 25 October 2017, available at <https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-scable-20171025.pdf>. Note also that Ms. Cable references her earlier, more comprehensive testimony before the Congress for further details on the Massachusetts data security requirements.

⁴² Testimony of Mike Litt, U.S. PIRG, before this committee, 25 October 2017, available at <https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-mlitt-20171025.pdf>

⁴³ Opening statement of Financial Services Committee Chairman Jeb Hensarling, 5 October 2017, available at: <https://financialservices.house.gov/news/documentsingle.aspx?DocumentID=402391>.

Testimony of Edmund Mierzwinski, U.S. PIRG, 1 Nov 2017

for a first violation of the rules; it can only impose penalties after an enforcement order is violated. The FTC has no authority to supervise firms, as the Consumer Bureau does. The Consumer Bureau has much broader rulemaking authority than the FTC.

5) Congress Should Enact Comprehensive FCRA Reforms, H.R. 3755, the Comprehensive Consumer Credit Reporting Reform Act (Waters) and Also Protect the Consumer Bureau

I first testified in favor of Fair Credit Reporting Act reform in 1989, before a predecessor subcommittee of the old House Banking Committee called Consumer Affairs and Coinage. While credit bureau reform has been a work in progress ever since then, we made major strides in 1996 and 2003. Then, with the establishment of the Consumer Bureau in 2010, which began supervising the larger bureaus in 2012, we have seen more advances. I concur with the detailed testimony by Chi Chi Wu on numerous occasions in support of further legislative reforms and urge the committee to pass HR 3755 as proposed by Ranking Member Waters. As Chi Chi Wu said to the full committee last week:

“Due to this insufficient regulation and the lack of consumer choice, the credit reporting agencies have grown up in a culture of impunity, arrogance, and exploitation. For decades, they have abused consumers, cut corners in personnel and systems, and failed to invest in measures that would promote accuracy or handle disputes properly.”⁴⁴

We concur. We also urge reconsideration of the majority’s views on the Consumer Bureau. It has done yeoman work for consumers, while being fully transparent in its efforts. It is needed now, more than ever.

6) Congress Should Allow Private Enforcement and Broad State and Local Enforcement of Any Law It Passes: The marketplace only works when we have strong federal laws and strong federal enforcement of those laws, buttressed by strong state and local and private enforcement.

Virtually all federal privacy or data security or data breach proposals specifically state that no private right of action is created. Such clauses should be eliminated and it should also be made clearer that the bills have no effect on any of the 17 state law private rights of action that apply to data security and breaches. Further, no bill should include language reducing the scope of state Attorney General or other state-level public official enforcement. Further, any federal law should not restrict state enforcement only to state Attorneys General, but allow enforcement by local enforcers, such as district attorneys.

7) Congress Should Address SSNs and authentication:

In the U.S., new account identity theft and other frauds, including tax refund fraud and medical services fraud, are fueled both by the high demand for “instant credit” and by that critical flaw in our credit granting system, where SSNs serve as both a matching identifier in databases and as an authenticator of a consumer applicant. The Social Security Number genie left the bottle years ago. While we would prefer that it not be used as a commercial identifier, in numerous databases, it is. The Congress needs to examine how to prevent it from being used as both an authenticator and an identifier. Your ATM card PIN is a secret authenticator. It is different from your bank account number and known only to you. Whether it is a two-factor authentication or some other solution, we need

⁴⁴ Testimony of Chi Chi Wu, National Consumer Law Center, before the committee on 25 October 2017, available at <https://financialservices.house.gov/uploadedfiles/hhrg-115-ba00-wstate-ccwu-20171025.pdf>

to move on from using Social Security Numbers for both identification and authentication because SSNs are not secret and don't do the job.⁴⁵

8) Congress should further investigate marketing of overpriced credit monitoring and identity theft subscription products:

Prices for credit monitoring, credit scoring and identity theft protection and remediation products from credit bureaus, banks and firms such as Lifelock range up to \$19.99/month or more. The marketing of the products, often based on scant 3-5 day free trial periods, is often deceptive. In 2017, the Consumer Bureau imposed fines totaling over \$23 million on both Equifax and Transunion over their marketing of credit scores and subscription credit monitoring services.⁴⁶

In 2005 and then again in 2007 the FTC had imposed a total of over \$1.2 million in fines on the credit bureau Experian's subsidiary Consumerinfo.com for deceptive marketing of its own various credit monitoring products; Experian had tied its expensive subscription product to the new free annual credit report required by law.⁴⁷

Banks receive massive commissions for selling these under-performing, over-priced products to their own customers. The Consumer Bureau has also imposed fines totaling about \$1.5 billion on big banks selling similar products, derived from consumer credit reporting products. While it is likely that those Consumer Bureau enforcement orders⁴⁸ against several large credit card companies for deceptive sale of the add-on products has caused banks to think twice about continuing these relationships with third-party firms, the committee should also consider its own examination of the sale of these credit card add-on products.

Lifelock, a major company in the identity protection space, was fined \$12 million in 2010 by the FTC and 35 states for deceptive marketing.⁴⁹

Then, in 2015, the FTC held Lifelock in contempt and fined it an additional \$100 million for failing to protect the security of its customers' files and falsely advertising that it had.⁵⁰

In his testimony before Congress, Richard Smith of Equifax admitted that Lifelock was a third-party partner of

⁴⁵ See "Security In Numbers: SSNs and Identity Theft," an FTC report, which discusses the problems of using Social Security Numbers to authenticate people even though they are not secret, but ubiquitous and widely available to thieves, December 2008, available at <https://www.ftc.gov/sites/default/files/documents/reports/security-numbers-social-security-numbers-and-identity-theft-federal-trade-commission-report/p075414ssnreport.pdf>

⁴⁶ Press release, "CFPB Orders TransUnion and Equifax to Pay for Deceiving Consumers in Marketing Credit Scores and Credit Products," 3 January 2017, available at <https://www.consumerfinance.gov/about-us/newsroom/cfpb-orders-transunion-and-equifax-pay-deceiving-consumers-marketing-credit-scores-and-credit-products/>

⁴⁷ Press release, "FTC Alleges Ads For "Free" Credit Report Violate Federal Court Order," 21 February 2007, available at <https://www.ftc.gov/news-events/press-releases/2007/02/consumerinfo-com-settles-ftc-charges>

⁴⁸ We discuss some of the CFPB add-on cases against bank marketing of subscription products here <https://ispirn.org/blogs/eds-blog/usp/cfpb-gets-results-consumersand-taxpayers-too>

⁴⁹ Press release, "LifeLock Will Pay \$12 Million to Settle Charges by the FTC and 35 States That Identity Theft Prevention and Data Security Claims Were False," 9 March 2010, available at <https://www.ftc.gov/news-events/press-releases/2010/03/lifelock-will-pay-12-million-settle-charges-ftc-35-states>

⁵⁰ "LifeLock to Pay \$100 Million to Consumers to Settle FTC Charges It Violated 2010 Order," 12 December 2017, available at <https://www.ftc.gov/news-events/press-releases/2017/12/lifelock-pay-100-million-consumers-settle-ftc-charges-it-violated>

the credit bureau.⁵¹

Consumers who want credit monitoring can monitor their credit themselves. No one should pay for it. You have the right under federal law to look at each of your 3 credit reports (Equifax, Experian and TransUnion) once a year for free at the federally-mandated central site annualcreditreport.com. Don't like websites? You can also access your federal free report rights by phone or email. You can stagger these requests – 1 every 4 months -- for a type of do-it-yourself no-cost monitoring. And, if you suspect you are a victim of identity theft, you can call each bureau directly for an additional free credit report. If you live in Colorado, Georgia, Massachusetts, Maryland, Maine, New Jersey, Puerto Rico or Vermont, you are eligible for yet another free report annually under state law by calling each of the Big 3 credit bureaus.

9) Any federal breach standard should not treat merchants differently than financial institutions:

Nearly every federal breach notification bill that requires breach notification by covered entities (regardless of its harm trigger or other provisions), seeks to provide a safe harbor to entities already covered by Title V of the Gramm-Leach-Bliley Act or other federal data security laws, such as those applicable to health care entities.⁵² As merchants and retailers have long pointed out, this leaves them, as non-financial institutions under the GLBA scheme, subject to notification standards higher than those of GLBA “financial institutions.” Such a two-tiered system makes no sense from a policy perspective. Of course, merchants have also suffered enmity from banks and credit unions which seek affirmative legislation holding them liable for breach costs. Such disputes should be covered in contract, not law.

III. Conclusion: A Threat to Consumers Is Posed by the Basic Business Model of the Digital Data Advertising Ecosystem

This testimony focuses primarily on the impact of a failure to secure consumer information. Congress should also investigate the broader problem of the over-collection of consumer information for marketing, tracking and predictive purposes. While the digital advertising ecosystem expands the number of vectors for misuse, the ubiquitous tracking of consumers as commodities or products poses threats as a business model itself.⁵³

In many ways, data breaches are the mere tip of the iceberg when it comes to privacy threats in the Big Data world. In the Big Data world, companies are collecting vast troves of information about consumers. Every day, the collection and use of consumer information in a virtually unregulated marketplace is exploding. New technologies allow a web of interconnected businesses – many of which the consumer has never heard of – to assimilate and share consumer data in real-time for a variety of purposes that the consumer may be unaware of and may cause consumer harm. Increasingly, the information is being collected in the mobile marketplace and includes a new level of hyper-localized information.

Contrast the FCRA with the new Big Data uses of information which may not be fully regulated by the FCRA. The development of the Internet marketing ecosystem, populated by a variety of data brokers, advertising

⁵¹ Tara Siegel Bernard, “The Post-Equifax Marketing Push: Identity Protection Services,” 25 October 2017, available at <https://www.nytimes.com/2017/10/25/your-money/identity-protection-equifax.html>

⁵² See the Health Insurance Portability and Accountability Act (HIPAA) (45 CFR Subpart C of Part 164).

⁵³ See Edmund Mierzwinski and Jeff Chester, “Selling Consumers, Not Lists: The New World of Digital Decision-Making and the Role of the Fair Credit Reporting Act,” 46 Suffolk University Law Review Vol. 3, page 845 (2013), available at http://suffolklawreview.org/wp-content/uploads/2014/01/Mierzwinski-Chester_Lead.pdf

Testimony of Edmund Mierzwinski, U.S. PIRG, 1 Nov 2017

networks and other firms that collect, buy and sell consumer information without their knowledge and consent, is worthy of much greater Congressional inquiry.⁵⁴ As I wrote, with a colleague from the Center for Digital Democracy:

“Dramatic changes are transforming the U.S. financial marketplace. Far-reaching capabilities of “Big-Data” processing that gather, analyze, predict, and make instantaneous decisions about an individual; technological innovation spurring new and competitive financial products; the rapid adoption of the mobile phone as the principal online device; and advances in e-commerce and marketing that change the way we shop and buy, are creating a new landscape that holds both potential promise and risks for economically vulnerable Americans.”⁵⁵

Conclusion:

Congress has largely failed to address numerous digital threats to consumers, from data breaches to data brokers running amok to the very architecture of the digital ecosystem, where nearly every company – known and unknown – is tracking consumers, building a dossier on them and even auctioning them off to the highest bidder in real time (for advertising or financial offers). Any data security, breach or privacy legislation should provide individuals with meaningful and enforceable control over the collection, use and sharing of their personal information.

Any bill should become a federal floor that upholds state privacy and data security laws, grants strong regulatory and enforcement authority to the Federal Trade Commission and state officials and allows states to continue to act as privacy leaders. Congress should give the Federal Trade Commission (FTC) adequate resources to protect privacy. Congress should defend the Consumer Bureau.

Any bill should adequately define what constitutes sensitive information, and provide consumers with meaningful choices about use of their data (ideally an opt-in to any secondary use). Any bill should protect large categories of personal information, including geolocation data, health records and marketing data collected on or off line. There should be no exceptions for business records, data “generally available to the public,” and cyber threat indicators.

Proposed bills should not give companies leeway to determine the protections that consumers will receive. Most proposed bills’ protections apply only if a company identifies a “context” or risk of harm. Protections should not be conditioned in such a way. Companies should face the threat of public exposure for failing to protect customer information. Companies should face monetary penalties to victims.

As Congress considers amendments to address all the issues highlighted in this testimony, from data breaches to data security to data brokers and the Internet advertising ecosystem, it needs to consider any reforms in the context of the strongest possible application of the Code of Fair Information Practices discussed above.

⁵⁴ See the FTC’s March 2012 report, “Protecting Consumer Privacy in an Era of Rapid Change: Recommendations For Businesses and Policymakers,” available at <https://www.ftc.gov/news-events/media-resources/protecting-consumer-privacy/ftc-privacy-report>

⁵⁵ Edmund Mierzwinski and Jeff Chester, “Big Data Means Big Opportunities and Big Challenges,” 27 March 2014, U.S. PIRG and the Center for Digital Democracy, available at <https://uspirg.org/reports/usfbig-data-means-big-opportunities-and-big-challenges>

Testimony of Edmund Mierzwinski, U.S. PIRG, 1 Nov 2017

It is important that policymakers understand that you cannot bifurcate the issues of data security and privacy. Consumer privacy is threatened when companies can buy or sell our information and we have little choice or control. Consumer privacy is threatened when data collectors do not keep data secure. In the new Big Data world, where firms are racing to vacuum up even more data than ever before, with even less acknowledgement of any privacy interest by consumers (or citizens), it is important that we re-establish norms that give consumers and citizens greater control over the collection, and use, of their personal information.

Thank you for the opportunity to provide the Committee with our views. We are happy to provide additional information to Members or staff.

—



Testimony of

Debra Schwartz

President & CEO

Mission Federal Credit Union

on behalf of

The National Association of Federally-Insured Credit Unions

“Data Security: Vulnerabilities and Opportunities for Improvement”

Before the

House Financial Services Subcommittee on Financial Institutions and Consumer Credit

November 1, 2017

Introduction

Good morning Chairman Luetkemeyer, Ranking Member Clay and Members of the Subcommittee. Thank you for the invitation to appear before you this morning. My name is Debra Schwartz and I am testifying today on behalf of the National Association of Federally-Insured Credit Unions (NAFCU). I am the President and CEO of Mission Federal Credit Union (Mission Fed), headquartered in San Diego, California, and also serve on NAFCU's Board of Directors as Treasurer.

Mission Fed is a federally chartered credit union serving those who live, work or attend school in San Diego County. We serve more than 219,000 members through 30 local branches, making Mission Fed the largest locally-based credit union exclusively serving San Diego County.

As you are aware, NAFCU is the only national organization exclusively representing the interests of the nation's federally-insured credit unions. NAFCU-member credit unions collectively account for approximately 70 percent of the assets of all federally-insured credit unions. It is my privilege to submit the following testimony on behalf of NAFCU, our credit unions and the 110 million credit union members they represent that have been heavily impacted by ongoing data security breaches through no fault of their own.

Credit Unions and Data Security

Today, my testimony will cover credit union efforts to maintain a successful track record of protecting member information, NAFCU's work on the data security front, the impacts of recent retailer and credit bureau data breaches on credit unions and consumers, including the financial

burdens they have faced. I will also outline NAFCU's principles for data security reform and potential legislative next steps to address consumer data threats that exist in the 21st century cyber environment.

As members of the committee are well aware, cyber and data crime has reached epic proportions in nearly all sectors of the economy. Symantec's *2016 Internet Security Threat Report* characterized 2016 as a year when "cyber attackers revealed new levels of ambition." According to the report, more than 1.1 billion identities were exposed in security breaches last year, which was nearly double the total from 2015. While large companies across all sectors are still a prime target for malware, the report notes that "small-to-medium sized businesses were the most impacted."

In a recent report by Javelin Strategy & Research, they found that card not present fraud increased by 40% from 2015 to 2016. The author of the report, Al Pascual, head of security, risk, and fraud at Javelin Strategy & Research noted that the jump in fraud was not simply the shift of card present to card not present fraud, but pointed to the online retailers and merchants not maintaining up-to-date security standards.

NAFCU supports comprehensive data and cybersecurity measures to protect consumers' personal data. Credit unions and other depository institutions already protect data consistent with the provisions of the 1999 *Gramm-Leach-Bliley Act* (GLBA) and are examined by a regulator for compliance with these standards. Unfortunately, there is no comprehensive regulatory structure similar to what GLBA put in place for depository institutions for other

entities that may handle sensitive personal and financial data. Too often, credit unions are left cleaning up the mess and helping their members restore their personal financial information after another entity has suffered a breach. Enough is enough. Something must be done.

In today's digital economy, data security poses a threat to businesses of all sizes, individual consumers, and even national security. Securing consumers' personal information and financial accounts will require the *entire* payments ecosystem to take an active role in addressing emerging threats, and in turn require all industries to be proactive in protecting consumers' personally identifiable and financial information from the onset. Congress must require this.

Credit unions have been able to successfully minimize emerging threats and data breaches. Still, consumers unintentionally put themselves at risk every time they use their debit or credit card. Given the magnitude of the many recent data breaches and the sheer number of consumers impacted, policy makers have a clear bipartisan opening to ensure all industries in the payments system have a meaningful federal data safekeeping standard and that is enforced to help prevent further breaches from occurring. Now is the time for Congress to act to create a national standard on data security for those who do not already have one.

Credit Unions and the *Gramm-Leach-Bliley Act*

GLBA and its implementing regulations have successfully limited data breaches among depository institutions and this standard has a proven track record protecting valuable information since its enactment in 1999. This record of success is why NAFCU believes any future requirements must recognize this existing national standard for depository institutions

such as credit unions. While credit reporting agencies, such as Equifax, are governed by some of the data security standards set forth by GLBA, they are not examined by a regulator for compliance with these standards in the same manner as depository institutions are under the act. This is an area that likely needs addressing.

Consistent with Section 501 of the GLBA, the National Credit Union Administration (NCUA) established administrative, technical and physical safeguards to ensure the (1) security, (2) confidentiality, (3) integrity, (4) and proper disposal of consumer information and other records. Under the rules promulgated by the NCUA, every credit union must develop and maintain an information security program to protect customer data. Additionally, the rules require third party service providers that have access to credit union data take appropriate steps to protect the security and confidentiality of the information.

NAFCU believes the best way to move forward and prevent data breaches is to create a comprehensive framework for industries that are not already subject to data security standards of regulatory oversight with the responsibility to protect consumer data they collect and enforcing those standards. Entities that are considered "GLBA institutions" should be regularly examined by a regulatory body. The oversight of credit unions, banks and other depository institutions is best left to the functional financial institution regulators that have experience in this field. It would be redundant at best and possibly counter-productive to authorize any agency—other than the prudential regulators—to promulgate new, and possibly duplicative or contradictory, data security regulations for financial institutions already in compliance with GLBA.

Below, I outline the key elements, requirements and definitions of the GLBA. Specifically, the GLBA:

- Requires financial institutions to establish privacy policies and disclose them annually to their customers, setting forth how the institution shares nonpublic personal financial information with affiliates and third parties.
- Directs regulators to establish regulatory standards that ensure the security and confidentiality of customer information.
- Permits customers to prohibit financial institutions from disclosing personal financial information to non-affiliated third parties.
- Prohibits the transfer of credit card or other account numbers to third-party marketers.
- Prohibits pretext calling, which generally is the use of false pretenses to obtain nonpublic personal information about an institution's customers.
- Protects stronger state privacy laws and those not inconsistent with these federal rules.
- Requires the U.S. Department of Treasury and other federal regulators to study the appropriateness of sharing information with affiliates, including considering both negative and positive aspects of such sharing for consumers.

Sensitive Consumer Information

Sensitive consumer information is defined as a member's name, address, or telephone number in conjunction with the member's social security number, driver's license number, account number, credit or debit card number, or personal identification number or password that would permit access to the member's account. Sensitive consumer information also includes any combination of components of consumer information that would allow someone to log into or access the

member's account, such as user name and password or password and account number. Under the guidelines, an institution must protect against unauthorized access to or use of consumer information that could result in substantial harm or inconvenience to any consumer.

Unauthorized Access to Consumer Information

The agencies published guidance to interpret privacy provisions of GLBA and interagency guidelines establishing information security standards. The guidance describes response programs, including member notification procedures, that a depository institution should develop and implement to address unauthorized access to or use of consumer information that could result in substantial harm or inconvenience to a member.

The security guidelines require every credit union to have an information security program designed to:

- Ensure the security and confidentiality of consumer information;
- Protect against any anticipated threats or hazards to the security or integrity of such information; and,
- Protect against unauthorized access to or use of such information that could result in substantial harm or inconvenience to a member.

Risk Assessment and Controls

The security guidelines direct every credit union to assess the following risks, among others, when developing its information security program:

- Reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration, or destruction of consumer information or consumer information systems;
- The likelihood and potential damage of threats, taking into consideration the sensitivity of consumer information; and,
- The sufficiency of policies, procedures, consumer information systems, and other arrangements to control for the risks to sensitive data.

Following the assessment of these risks, the security guidelines require a credit union to design a program to address the identified risks. The particular security measures an institution should adopt depend upon the risks presented by the complexity and scope of its business. This is a critical aspect of GLBA that allows flexibility and ensures the regulatory framework is applicable for the largest and smallest in the financial services arena. As the committee considers data security measures, it should be noted that scalability is achievable and that it is inaccurate when other industries claim they cannot have a federal data safekeeping standard that could work across a sector of varying sized businesses.

At a minimum, the credit union is required to consider the specific security measures enumerated in the Security Guidelines, and adopt those that are appropriate for the institution, including:

- Access controls on consumer information systems, including controls to authenticate and permit access only to authorized individuals and controls to prevent employees from

providing consumer information to unauthorized individuals who may seek to obtain this information through fraudulent means;

- Background checks for employees with responsibilities for access to consumer information;
- Response programs that specify actions to be taken when the institution suspects or detects that unauthorized individuals have gained access to consumer information systems, including appropriate reports to regulatory and law enforcement agencies;
- Train staff to implement the credit union's information security program; and,
- Regularly test the key controls, systems and procedures of the information security program. The frequency and nature of such tests should be determined by the credit union's risk assessment. Tests should be conducted or reviewed by independent third parties or staff independent of those that develop or maintain the security programs.”

Service Providers

The security guidelines direct every credit union to require its service providers through contract to implement appropriate measures designed to protect against unauthorized access to, or use of, consumer information that could result in substantial harm or inconvenience to any consumer.

Third-party providers are very popular for many reasons, most frequently associated with cost-savings/overhead reduction. However, where costs may be saved for overhead purposes, they may be added for audit purposes. Because audits typically are annual or semi-annual events, cost savings may still be realized but the risk associated with outsourcing must be managed regardless of cost. In order to manage risks, they must first be identified.

A credit union that chooses to use a third-party provider for the purposes of information systems-related functions must recognize that it must ensure adequate levels of controls so the institution does not suffer the negative impact of such weaknesses.

Response Program

Every credit union must develop and implement a risk-based response program to address incidents of unauthorized access to consumer information. A response program should be a key part of an institution's information security program. The program should be appropriate to the size and complexity of the institution and the nature and scope of its activities.

In addition, each institution should be able to address incidents of unauthorized access to consumer information in consumer information systems maintained by its service providers. Where an incident of unauthorized access to consumer information involves consumer information systems maintained by an institution's service providers, it is the responsibility of the financial institution to notify the institution's consumers and regulator. However, an institution may authorize or contract with its service provider to notify the institution's consumers or regulator on its behalf.

Consumer Notice

Timely notification to members after a security incident involving the unauthorized access or use of their information is important to manage an institution's reputation risk. Effective notice may also mitigate an institution's legal risk, assist in maintaining good consumer relations, and enable the institution's members to take steps to protect themselves against the consequences of identity

theft. This is one area that Equifax appears to have failed in light of the recent breach. A regulator overseeing and examining their programs would have likely made sure that they had a timely notification plan in place.

Content of Consumer Notice

Consumer notice should be given in a clear and conspicuous manner. The notice should describe the incident in general terms and the type of consumer information that was the subject of unauthorized access or use. It should also generally describe what the institution has done to protect consumers' information from further unauthorized access. In addition it should include a telephone number that members can call for further information assistance. The notice should also remind members of the need to remain vigilant over the next 12 to 24 months, and to promptly report incidents of suspected fraud or identity theft to the institution.

Delivery of Consumer Notice

Notice should be delivered in any manner designed to ensure that a consumer can reasonably be expected to receive it.

Regulators Oversight of Financial Sector Data Security

Since the passage of GLBA, financial regulators have developed robust guidance to help institutions develop information security programs and enterprise risk management policies to address data and cybersecurity needs. In addition, financial regulators oversee bank and credit union data security through periodic examinations designed to assess the risks associated with IT

environments of varying size and complexity. Currently, credit bureaus are not regularly examined for adherence to data security standards by a regulatory body.

Guidance promulgated by the Federal Financial Institutions Examination Council (FFIEC) has shaped the contents of bank and credit union examinations. In June 2015, the FFIEC publicly announced its Cybersecurity Assessment Tool (CAT), which was influenced in large part by the Framework for Improving Critical Infrastructure Cybersecurity (the Framework), released by the National Institute of Standards and Technology (“NIST”) in 2014. Both the Framework and the CAT are voluntary tools that credit unions and banks can use to gauge their cybersecurity readiness. The Framework has endowed the CAT with a common lexicon of cybersecurity terminology, which has also influenced the thinking of other financial institution regulators. Furthermore, NCUA has said that its ongoing update of IT examination procedures will adhere to the principles described in the CAT, and other financial regulators have either aligned their cybersecurity standards more closely with the Framework or voiced support for its risk-based approach.

Financial sector data security has always been a priority for banking and credit union regulators; however, in recent years it has emerged as top issue. NCUA has made cybersecurity a supervisory priority since 2013, and the agency reminded credit unions in 2016 that “technological innovation, the expansion of social networking and growing interconnectivity are fueling fundamental change in cybersecurity procedures and processes.” NCUA forecasts that elevated risk levels may lead to “higher mitigation costs and lower consumer confidence, as well as greater financial and legal risks.” Likewise, other regulators have either announced changes to

their own examination procedures as a result of growing technological complexity in the financial sector, or issued new proposals aimed at mitigating unprecedented levels of data security risk.

Protecting Consumer Data is Important

With the increase of massive data security breaches, from the Target breach at the height of holiday shopping in 2013 impacting over 110 million consumer records to the recent Equifax breach impacting up to 143 million consumers (43 percent of the U.S. population) Americans are becoming more aware and more concerned about data security and its impact. A recent Gallup poll found that 69 percent of U.S. adults are frequently or occasionally concerned about having their credit card information stolen by hackers, while a 2016 Gallup survey reported that 27 percent of Americans say they or another household member had information from a credit card used at a store stolen in the last year. These staggering survey results speak for themselves and should cause serious pause among lawmakers on Capitol Hill.

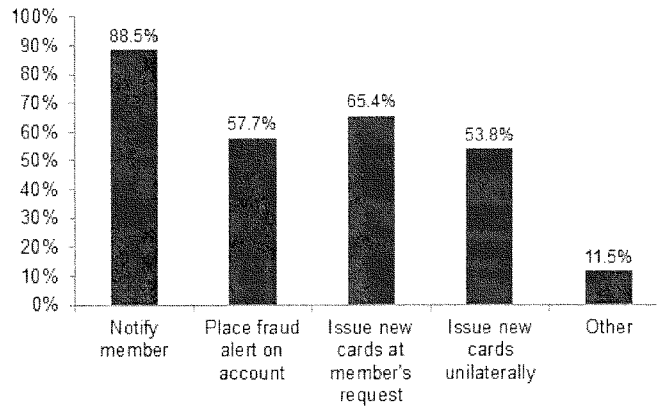
Since the Target and Home Depot breaches, which brought large scale data breaches to light, there have been many others varying by industry, including the most recent Equifax and Yahoo breaches. Data security breaches are not just a retailer problem, but occur across many industries. This highlights the need for a comprehensive national data security standard to protect data akin to what is in place for depository institutions under GLBA.

Data security breaches are more than just an inconvenience to consumers as they wait for their debit and/or credit cards to be reissued. Breaches often result in compromised card information

leading to fraud losses, unnecessarily damaged credit ratings, and even identity theft. Symantec's *Internet Security Threat Report* issued in April of 2016 found that individuals' financial information was exposed in 33% (over 140 million) of the 429 million records compromised in the 2015 breaches. That percentage is up significantly from 18% in 2013. More than 23% of the US population had their financial identities compromised by a data breach in 2014.

While the headline grabbing breaches are certainly noteworthy, the simple fact is that data breaches throughout our nation are happening almost every day. A survey of NAFCU member credit unions in June 2017, found that respondents were alerted to potential breaches an average of 189 times in 2016. Over 40 percent of the respondents said that they saw an increase in these alerts from 2015, while only 14 percent reported a decrease. When credit unions are alerted to breaches, they take action to respond and protect their members. The chart below outlines the actions that credit unions took to respond to data breaches in 2014.

In response to 2014 merchant data breaches, what actions did you take?



Source: NAFCU *Economic & CU Monitor* survey

Credit unions suffer steep losses in re-establishing member safety after a data breach occurs. They are often forced to charge off fraud-related losses, many of which stem from a negligent entity's failure to protect sensitive financial and personal information or the illegal maintenance of such information in their systems. Moreover, as many cases of identity theft have been attributed to data breaches, and as identity theft continues to rise, any entity that stores financial or personally identifiable information should be held to minimum federal standards for protecting such data.

Every entity collecting and storing consumers' personal and financial information regardless of industry are targets of cyberattacks. The difference, however, is that credit unions have been required to develop and maintain robust internal protections to combat these attacks and are

required by federal law and their regulator to protect this information as well as notify their members when a breach occurs that puts them at risk. As outlined above, every credit union must comply with significant data security regulations, and undergo regular examinations to ensure that these rules are followed. A credit union faces potential fines of up to \$1 million per day for compliance violations. These extensive requirements and safeguards discussed earlier in my testimony have evolved along with cyber threats and technological advances and have been enhanced through regulation since they were first required in 1999. Entities that are considered "GLBA institutions" should be regularly examined by a regulatory body. This includes national credit bureaus such as Equifax, which are not currently examined.

A credit union data security program to protect its own system can have many security components, such as:

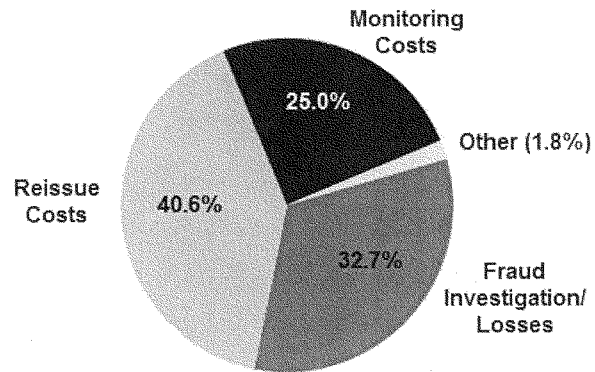
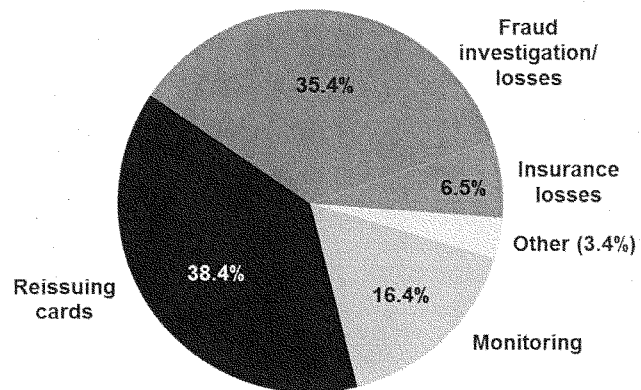
1. Firewall (including redundant and internal firewalls)
2. Intrusion Prevention
3. Botnet Filtering
4. Anti-Virus protection
5. Malware protection
6. Management and Monitoring Services
7. Anti-Phishing and Phishing site takedown services
8. Third party vulnerability assessments and testing
9. Web Filter
10. Spam Filter
11. Secure Email

12. Encryption

13. End point security

These elements can have a significant cost to the institution. A February, 2015, survey of NAFCU members found that the average respondent credit union spent \$136,000 on data security measures in 2014, which does not even factor in the additional costs that the credit union faced due to data breaches at other entities. At Mission Fed, we have already spent over \$1 million in 2017 to protect our members, including hardware and software updates for the encryption of data, and DDoS protection and testing. This does not even include internal staff costs.

The ramifications of recent data breaches for credit unions and their members have been monumental. The July 2017 survey of NAFCU members found that the estimated costs associated with merchant data breaches in 2016 were \$362,000 on average per credit union. Almost all respondents noted that merchant data breaches lead to increased member-service costs and needs that are not reflected in these direct costs. The three main elements of these costs were card reissuing costs, fraud investigations/losses and account monitoring. The chart on the next page outlines how these various costs from merchant data breaches are broken down.

Percent of Fraud-Related Costs in 2014**Share of CU Fraud-Related Costs in 2016**

Source: NAFCU *Economic CU Monitor* survey (July 2017)

Another cost, though difficult to measure, is that members often do not know that their compromised cards are due to a specific data breach. The card networks do not identify the compromise sources in their card alerts. Therefore, credit union staffs typically can only inform affected members that their cards may be compromised, not the source of the compromise. For all the members know, the source of the problem may be the credit union itself. I hear from many of my tellers that members sometimes question the credit union's security when their information is compromised. This undoubtedly can have an unjustified but damaging effect on their confidence in their credit union.

Additionally, one of the residual effects that goes largely unnoticed is the impact that the reissuance of a card has on the neural network of a credit union. This is a credit union's own fraud detection system. Some of the components of the system are payment patterns and history of card usage, as is the case with most neural networks. Every time a credit union has to reissue a card, the pattern and history for that member is erased and it starts over. This increases the chance that the member will make a purchase that is perfectly acceptable, but get denied because the network does not recognize that what they are doing is perfectly normal. This is especially true for credit union members who travel.

Unfortunately, credit unions often never see any reimbursement for their costs associated with the majority of data breaches. Even when there are recoupment opportunities, such as the recent Target settlement with MasterCard, it is usually only pennies on the dollar in terms of the real costs and losses incurred. Meanwhile, those that were negligent in recent data security breaches are posting record profits. A 2015 Columbia University review of financial statements of

merchants reveals that retailers barely notice a financial hit from massive data breaches. At Mission Fed, we have seen over \$1.7 million in card fraud already in 2017 and have incurred \$6.3 million in card fraud since 2013. Because insurance costs have risen so high, we self-insure, so this is money that ultimately impacts our ability to make loans or provide programs to our members.

At Mission Fed, we participate in MasterCard's Account Data Compromise (ADC) Program which notifies us of events where our members' cards have been involved in a security breach. Since January 2013, we have received nearly 1,400 ADC notifications from MasterCard affecting our cardholders.

Mission Fed takes cardholder security seriously, so we choose to reissue new cards to members anytime a member's card appears on an ADC event notice. Since January 2013, we have reissued over 146,000 cards as a result of ADC notifications. To put that in perspective, we have approximately 280,000 cards issued to our members, so more than 50% have been replaced as a result of a compromise. This number does not include card replacements due to member reported fraud, as we always block cards involved in fraud reported by members.

Payment networks are critical partners to credit unions in ensuring credit union members have the credit and debit card programs they need and demand. Collectively, the networks have worked together to standardize the Payment Card Industry (PCI) Data Security Standard designed to provide merchants and retailers with a framework of specifications, tools, measurements and support resources to ensure the safe handling of cardholder information.

While NAFCU appreciates the positive progress in this regard, credit unions and other issuers are still seeing steep losses in the wake of data breaches and would like to see the networks do everything they can to make reimbursement in the wake of fraud stemming from a data breach more equitable. As discussed, NAFCU believes the negligent entity should be wholly responsible for such damages.

NAFCU's Key Data Security Principles

NAFCU has long been active on the data security front, and was the first financial services trade association to call for Congressional action in the wake of the 2013 data breach at Target. Recognizing that a legislative solution is a complex issue, NAFCU's Board of Directors has also established a set of guiding principles to help define key issues credit unions would like to see addressed in any comprehensive cyber and data security effort that may advance. These principles include:

- **Payment of Breach Costs by Breached Entities:** NAFCU asks that credit union expenditures for breaches resulting from card use be reduced. A reasonable and equitable way of addressing this concern would be to enact legislation to require entities to be accountable for costs of data breaches that result on their end, especially when their own negligence is to blame.
- **National Standards for Safekeeping Information:** It is critical that sensitive personal information be safeguarded at all stages of transmission. Under the GLBA, credit unions and other depository institutions are required to meet certain criteria for safekeeping

consumers' personal information and are held accountable if that criteria is not met through examination and penalties. Unfortunately, there is no comprehensive regulatory structure akin to the GLBA that covers other entities who collect and hold sensitive information. NAFCU strongly supports the passage of legislation requiring any entity responsible for the storage of consumer data to meet standards similar to those imposed on depository institutions under the *GLBA*.

- **Data Security Policy Disclosure:** Many consumers are unaware of the risks they are exposed to when they provide their personal information. NAFCU believes this problem can be alleviated by simply requiring merchants to post their data security policies at the point of sale if they take sensitive financial data. Such a disclosure requirement would come at little or no cost to the merchant but would provide an important benefit to the public at large.
- **Notification of the Account Servicer:** The account servicer or owner is in the unique position of being able to monitor for suspicious activity and prevent fraudulent transactions before they occur. NAFCU believes that it would make sense to include entities such as financial institutions on the list of those to be informed of any compromised personally identifiable information when associated accounts are involved.
- **Disclosure of Breached Entity:** NAFCU believes that consumers should have the right to know which business entities have been breached. We urge Congress to mandate the

disclosure of identities of companies and merchants whose data systems have been violated so consumers are aware of the ones that place their personal information at risk.

- **Enforcement of Prohibition on Data Retention:** NAFCU believes it is imperative to address the violation of existing agreements and law by those who retain payment card information electronically. Many entities do not respect this prohibition and store sensitive personal data in their systems, which can be breached easily in many cases.
- **Burden of Proof in Data Breach Cases:** In line with the responsibility for making consumers whole after they are harmed by a data breach, NAFCU believes that the evidentiary burden of proving a lack of fault should rest with the negligent entity who incurred the breach. These parties should have the duty to demonstrate that they took all necessary precautions to guard consumers' personal information but sustained a violation nonetheless. The law is currently vague on this issue, and NAFCU asks that this burden of proof be clarified in statute.

Preventing Future Breaches

NAFCU has long argued that protecting consumers and financial institutions by preventing future data breaches hinges on establishment of strong federal data safekeeping standards for entities akin to what credit unions already comply with under the GLBA.

The time has come for Congress to enact a national standard on data protection for consumers' personal financial information. Such a standard must recognize the existing protection standards that depository institutions have under the GLBA and ensure the costs associated with a data breach are borne by those who incur the breach. Once again, all "GLBA institutions," including credit bureaus, should be subjected to examinations by a regulatory body as depository institutions already are. Additionally, consumers whose personal and financial data has been compromised have a right to be notified in a timely manner. This is where Equifax failed by waiting weeks to notify the public, including credit unions, of their breach. Unfortunately, Equifax's silence left the door open for more damage to be done from fraud. Depository institutions servicing the accounts should be made aware of any breach at a national credit bureau as soon as practicable so they can proactively monitor affected accounts, and any notification requirements should be enforced by a regulator. Congress needs to act to make this happen.

While some have said that voluntary industry standards should be the solution, the *Verizon 2015 Payment Card Industry Compliance Report* found that 4 out of every 5 global companies fail to meet the widely accepted Payment Card Industry (PCI) data security standards for their payment card processing systems. In fact, Verizon found that out of every data breach they studied over the 10 year study, not one single company was in compliance with the PCI standards at the time of the breach.

In addition, the report finds that the use of EMV cards ("chip cards") in other countries has not been a silver bullet solution to preventing fraudulent activity, but merely displaces it. The report

shows that once EMV use increases, criminals shift their focus to card not present transactions, such as online shopping. At Mission Fed, we have found that the EMV shift has done little to stem the increasing tide of fraud. While some argued for the “chip card” solution, the reality is that it is not a panacea and does not replace a sound data security standard.

One basic but important concept to point out with regard to almost all data and cyber threats is that a breach may never come to fruition if an entity handling sensitive information limits the amount of data collected on the front end and is diligent in not storing sensitive personal and financial data in their systems. Enforcement of prohibition on data retention cannot be over emphasized and it is a cost effective and commonsense way to cut down on emerging threats. If there is no financial data to steal, it is not worth the effort of cyber criminals.

Legislative Solutions

NAFCU believes that the best legislative solution so far on the issue of data security is the bipartisan legislation that was introduced in the 114th Congress by Representatives Randy Neugebauer and John Carney. The legislation, H.R. 2205, the *Data Security Act of 2015*, would have set a national data security standard that recognized those who already have one under the GLBA. We were pleased to see the bill get bipartisan support in this Committee in the last Congress and urge you to reintroduce and consider this legislation in this Congress.

As the committee is aware, the cyber and data security discussions cross the jurisdiction of several Congressional committees. The House Energy and Commerce Committee also advanced its own version of a data security bill in the last Congress. We would urge the Committee to

work with leaders on that Committee to craft a package that can get bipartisan support in both Committees. There have been industry discussions underway amongst interested groups and we would urge the Committee to work with industry to introduce and advance a package to create a robust national data security standard that can be enacted into law. The time for action is now.

We would also like to express our support for Title I of H.R. 4028, the *PROTECT Act of 2017*, offered by Representative McHenry, which would subject the credit bureaus to supervision and examination by the FFIEC. This would help address some of the concerns about the regulation of credit bureaus that I outlined earlier in my testimony. However, we believe other aspects of the bill, including Title III's phase-out of the credit bureau's use of Social Security Numbers, need further study for potential broader negative unintended impacts.

Conclusion

Data security, ensuring member safety, and how to incentivize and emphasize data safekeeping in every link of the payments chain is a top challenge facing the credit union industry today. Given the breadth and scope of many data breaches, we have reached a tipping point in the public dialogue about how to tackle these issues. NAFCU member credit unions and the 110 million credit union members across the country are looking to Congress to address data security issues and move forward with meaningful legislation that will make a difference to consumers. It is time to level the playing field and require equal data security treatment to all those who collect and store personally identifiable and financial data.

Consumers will only be protected when every sector of industry is subject to robust federal data safekeeping standards that are enforced by corresponding regulatory agencies. It is with this in mind that NAFCU urges Congress to modernize data security laws to reflect the complexity of the current environment and insist that entities collecting and storing personal financial information adhere to a strong federal standard in this regard.

Thank you for the opportunity to appear before you today on behalf of NAFCU. I welcome any questions you may have.



November 1, 2017

Chairman Blaine Luetkemeyer
 Financial Institutions & Consumer Credit Subcommittee
 House Financial Services Committee
 2230 Rayburn House Office Building
 Washington, DC 20515

Ranking Member Wm. Lacy Clay
 Financial Institutions & Consumer Credit Subcommittee
 House Financial Services Committee
 2428 Rayburn House Office Building
 Washington, DC 20515

Dear Chairman Luetkemeyer and Ranking Member Clay,

Food Marketing Institute (FMI) respectfully requests for this letter to be entered into the record for the hearing in the House Financial Services Committee Subcommittee on Financial Institutions and Consumer Credit hearing entitled, "Data Security: Vulnerabilities and Opportunities for Improvement." FMI proudly represents America's food retail and wholesale industry. Customer safety is one of the supermarket industry's top priorities. From the safety of the food we sell to the safety and security of our customers and their payment and shopping data, the grocery industry is committed to protecting our customers.

With this guiding principle, FMI is fully committed to the enactment of a federal data security standard and breach notification law that will replace the current inconsistent and confusing patchwork of varying state laws. Creating one national standard will help ensure individuals' sensitive information is protected regardless of geography and that consumers are effectively notified of a breach in a timely manner.

As Congress considers a possible federal breach notification or data security standards, FMI would like to share our priorities and offer our commitment to work with members of Congress to pass meaningful legislation.

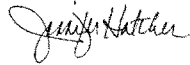
1. Establish a reasonable data security standard. Legislation that requires an entity to establish reasonable data security standards allows for adjustments and improvements as new technologies come on the market to address emerging threats. In addition, broad language provides flexibility and customization of protocols by industry and size of company. While existing federal regulation from other laws, such as the Health Insurance Portability and Accountability Act (HIPAA), and other existing industry standards should inform data security legislation, it does not make sense to take current guidelines written for one unique industry and codify them for industries they were not intended to cover, essentially creating a "one-size-fits-noone" scenario. Data security legislation will cover a broad array of industries and companies of all sizes. Using reasonable and customizable data security measures as the standard will give the Federal Trade Commission (FTC) clear authority to enforce with the ability to consider an individual industry's needs.
2. The breached party should be the default notice provider. The entity that is victim to a breach should be the one to provide notice to the consumer whose information was compromised. Many companies determine under contract who will notify in the event of a breach. FMI supports allowing flexibility to continue should the non-breached party elect to notify consumers, but liability for doing so should not automatically shift.
3. Any data security and breach notification legislation must be narrowly tailored to address the unlawful acquisition of information that would result in identity theft, financial or economic harm to an individual.

4. The FTC and any other federal agency enforcement authority must be clearly defined and limited within the constructs of the bill. FTC rulemaking authority should not be necessary for an effective federal data security and breach notification standard.
5. Entities that have been victims of a breach should not be subjected to crippling fines. Breached entities should be given the chance to remedy the situation by taking corrective measures following the first event before facing FTC fines.
6. Data security and breach notification legislation should be narrowly focused and should not include extraneous or controversial language that will stifle support for passage or effective implementation.
7. Strong state preemption is essential for any federal data security and breach notification standard to be successful. Without it, federal legislation will only add to the confusion of the current situation.

As the committee considers data security and breach notification legislation FMI asks for it to consider the current landscape, including existing FTC authority and previous actions taken, civil liabilities retailers already face when they are a victim of a breach and the fees and fines already levied by the major card brands following a breach.

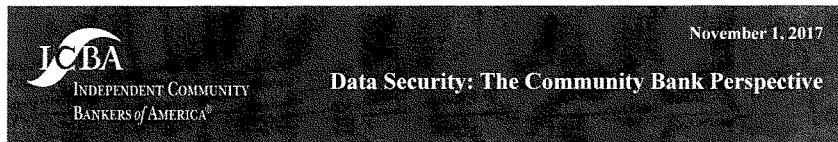
FMI members and staff stand ready to work with Congress to pass meaningful data security and national data breach notification legislation that will offer additional protection to our customers and consistency to our companies following this parameters. Please contact Hannah Walker, Senior Director, Technology and Nutrition Policy, at hwalker@fmi.org or 202-220-0630.

Sincerely,



Jennifer Hatcher
Chief Public Policy Officer & Senior Vice President
Government Relations

Cc: Members of the House Financial Services Committee Subcommittee on Financial Institutions & Consumer Credit.



On behalf of the more than 5,700 community banks represented by ICBA, we thank Chairman Luetkemeyer, Ranking Member Clay, and members of the Financial Services Subcommittee on Financial Institutions and Consumer Credit for convening today's hearing on "Data Security: Vulnerabilities and Opportunities for Improvement." The recent breach at Equifax highlights the urgent need for regulatory reforms to strengthen our payments and financial systems and deter future breaches. ICBA is pleased to have this opportunity to offer this statement for the hearing record.

Community banks are committed to safeguarding customer data and personal information. The community bank business model is founded on customer trust and service. Data security is a business imperative in the digital marketplace. Community banks invest significant and increasing resources in security controls to protect their consumers' data and critical systems.

ICBA and community bankers were appalled to learn of the massive data breach at Equifax involving 145.5 million American consumers. This breach has the potential to shake consumer confidence in our payments and financial systems for years. We urge Congress to take aggressive action to deter future breaches and mitigate the harm to consumers and to the financial system when breaches occur.

Examination and Supervision of Credit Reporting Agencies

Like financial institutions, the credit rating agencies (CRAs) are subject to the data security standards of the Gramm-Leach-Bliley Act (GLBA). Unlike financial institutions, CRAs are not examined or supervised for their compliance with these standards. This is a critical vulnerability. Significant third-party vendors that serve financial institutions are already subject to examination and supervision for compliance with GLBA standards. By the same logic, CRAs should be examined and supervised.

Create Incentives to Strengthen Data Security

Changes should not be limited to the CRAs but should extend to all entities that store personally identifiable consumer and financial data. Bad actors will continue to look for weaknesses in every link in the chain and future breaches will occur. To strengthen any weak links, ICBA recommends creating a legal structure in which the entity that incurs a breach – be it a retailer, CRA, financial institution, or other entity – bears liability for the cost of the breach.

When a breach occurs at any point in the chain, banks take a variety of steps to protect the integrity of their customers' accounts, including monitoring for indications of suspicious activity, changing customer identity procedures, responding to customer inquiries, reimbursing customers for confirmed fraudulent transactions, modifying customer limits to limit fraud losses, and blocking and reissuing cards of affected account holders at an estimated expense of up to \$15 per card. Banks willingly bear these costs up front because prompt action following a breach is essential to protecting the integrity of customer accounts. But these costs should ultimately be borne by the entity that incurs the breach. This is not only a matter of fairness; a liability shift is needed to properly align



incentives for entities that store consumer financial and personally identifiable data to strengthen their data security. When breaches have a material impact on entities bottom line, they will quickly become more effective at avoiding them.

Additional Reforms

In addition to the reforms noted above, we urge Congress to consider comprehensive solutions which would include the following legal and regulatory changes:

- All participants in the payments and financial system, including merchants and CRAs, and all entities with access to customer financial information, should be subject to Gramm-Leach-Bliley Act-like data security standards and examined for compliance with those standards.
- Barring a shift in liability to the breached entity (as recommended above), community banks should continue to be able to access various cost recovery options after a breach.
- ICBA supports a national data security breach and notification standard to replace the current patchwork of state laws.
- Community banks should be notified of a potential and/or actual breach as expeditiously as possible in order to mitigate losses.

Unintended Consequences Must Be Avoided

ICBA is eager to work with this committee on constructive proposals to strengthen data security. In evaluating proposals, we ask this committee to be mindful of unintended consequences that could result for consumers, community banks, and the payments and financial systems. These systems are highly complex, and the consequences of ill-considered policies are hard to predict.

Closing

Thank you again for convening today's hearing. Data breaches are among the highest concerns of America's community bankers. ICBA looks forward to continuing to work with the committee to promote customer security and protect against costly and damaging data breaches.

November 1, 2017

The Honorable Blaine Luetkemeyer
Chairman
Subcommittee on Financial Institutions
and Consumer Credit
Washington, D.C. 20515

The Honorable William Lacy Clay
Ranking Member
Subcommittee on Financial Institutions
and Consumer Credit
Washington, D.C. 20515

Dear Chairman Luetkemeyer and Ranking Member Clay:

Data security breaches continue to put millions of consumers at risk, and protecting consumer information is a shared responsibility of all parties involved. That is why the undersigned financial organizations and our members have supported comprehensive data protection and consumer notification legislation across several Congresses and have worked closely with key Members of this Committee and many others in the House and Senate to help advance this worthy cause.

Stopping incidents like the recent Equifax, Sonic, Hyatt and other breaches is critical for consumers, and also important to our members who often have the closest relationships with those affected. Data breaches impose significant costs on financial institutions of all sizes because our first priority is to protect consumers and make them whole. Our members provide relief to victims of breaches, regardless of where the breach occurs.

In our view, it is critical for Congress to move forward on legislation that puts in place one strong national data security and breach notification standard eliminating the current inconsistent patchwork of state law.

This standard should:

- 1) Ensure that all entities are required to protect sensitive personal and financial data;
- 2) In the event of a breach, require timely notification of consumers and impacted parties that are at risk; and
- 3) Ensure compliance via appropriate Federal and State regulators and eliminate overlapping and inconsistent laws and regulations.

Any legislation enacted into law must ensure that all entities that handle consumers' sensitive financial data have in place a robust process to protect data, which can help prevent breaches from happening in the first place. This standard should apply to all industries that handle sensitive information and would provide meaningful and consistent protection for consumers nationwide.

Our existing payments system serves hundreds of millions of consumers, retailers, financial institutions and the economy well. Protecting this system is a shared responsibility of all parties

involved and we must work together and invest the necessary resources to combat increasingly sophisticated threats to the payments system.

We look forward to working with you on this important issue.

Sincerely,

American Bankers Association
Consumer Bankers Association
Credit Union National Association
Financial Services Roundtable
Independent Community Bankers of America
National Association of Federally-Insured Credit Unions
The Clearing House

cc: Members of the House Subcommittee on Financial Institutions and Consumer Credit

XAVIER BECERRA
Attorney General

State of California
DEPARTMENT OF JUSTICE



Prepared Statement of Eleanor Blume
Special Assistant to California Attorney General Xavier Becerra
California Department of Justice

To the House Financial Services Committee

November 1, 2017

I applaud the attention being paid to the need for robust consumer privacy protections and am pleased to provide this statement for the record concerning data security and breach notification.

The recent breach at consumer reporting agency Equifax that affected 145 million Americans, including more than 15 million Californians, underscores the importance of vigorous state privacy protections and state enforcement of consumer protection laws.

Immediately following reports of the breach at Equifax, the California Attorney General's Office contacted Equifax, raised concerns about the mandatory arbitration provision and certain features of the company's consumer-facing website that created barriers to consumers accessing protections following the breach. In response to this engagement by our office, Equifax removed the arbitration provision and redesigned the website. Our team continues to work to get to the bottom of what happened and to evaluate all legal options to hold Equifax accountable for its actions and prevent this sort of breach—and the unacceptable response to it—from happening in the future. In addition, Attorney General Becerra issued several consumer alerts advising Californians on how to protect themselves in the wake of the Equifax breach and also contacted the other two national consumer reporting agencies, urging TransUnion and Experian to waive the fee for consumers to place a credit freeze on their accounts.¹

¹ See, *Attorney General Becerra Issues Consumer Alert Following Equifax Data Breach* (September 10, 2017), available at <https://oag.ca.gov/news/press-releases/attorney-general-becerra-issues-consumer-alert-following-equifax-data-breach>; *Attorney General Becerra Continues Efforts to Address Equifax Data Breach, Urges Consumers to Take Action to Protect Against Identity Theft* (September 15, 2017), available at <https://oag.ca.gov/news/press-releases/attorney-general-becerra-continues-efforts-address-equifax-data-breach-urges>; *In Wake of Equifax Data Breach, Attorney General Becerra Urges Credit Agencies to Provide Free Credit Freezes* (October 10, 2017), available at <https://oag.ca.gov/news/press-releases/wake-equifax-data-breach-attorney-general-becerra-urges-credit-agencies-provide>.

Prepared Statement of Eleanor Blume
 Special Assistant to Attorney General Xavier Becerra
 November 1, 2017
 Page 2

While the Equifax breach has, rightly, occupied headlines over the past couple of months, our office has consistently led the nation when it comes to protecting consumer privacy. Our privacy laws serve as models for other states' laws on privacy policies, Social Security number

confidentiality, and student data privacy. In 2003, California became the first state in the country to enact a data breach notification law.² Today, nearly every state has enacted similar laws, providing legal protection for the overwhelming number of Americans in the event of data breach.

California's statutory framework for privacy protection includes two critical pieces.

First, California law requires that businesses that collect personal information provide reasonable data security for that information. This means that a business that owns, licenses, or maintains personal information about a California resident is required under state law to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, and to protect the personal information from unauthorized access, destruction, use, modification, or disclosure.³ The obligation to protect personal information covers a number of sensitive types of information including name plus Social Security number, driver's license or identification card number, financial account information, medical information, or health insurance information; or user credentials that would permit access to an online account.

Second, in the event of a data breach, companies must notify victims of the breach expeditiously and without unreasonable delay. This means that any person, business, or state agency that does business in the state and owns or licenses computerized data that contains personal information must notify California victims whose unencrypted personal information was acquired, or reasonably believed to have been acquired, by an unauthorized person.⁴

The California Attorney General's Office is committed to holding businesses accountable for data security failures and to achieving remedies that help to prevent these sorts of breaches from happening in the future. When breaches cross state lines, much of this work happens on a collaborative, multistate basis including state attorneys general from across the country. For example, in May of this year, our office reached a multistate settlement with Target over its breach of payment card information for 40 million customers.⁵ And in September, we announced a settlement with Lenovo resolving allegations that the company illegally preinstalled ad-

² California Civil Code Sections 1798.29, 1798.82, and 1798.84 (amended by Stats. 2002, c. 915 (S.B. 1386), operative July 1, 2003).

³ California Civil Code s. 1798.81.5.

⁴ California Civil Code s. 1798.29(a), 1798.82(a).

⁵ *Attorney General Becerra: Target Settles Record \$18.5 Million Credit Card Data Breach Case*, available at <https://oag.ca.gov/news/press-releases/attorney-general-beccerra-target-settles-record-185-million-credit-card-data>.

Prepared Statement of Eleanor Blume
 Special Assistant to Attorney General Xavier Becerra
 November 1, 2017
 Page 3

injecting software that compromised the security of its computers, exposing consumers' sensitive personal information.⁶ In both of these judgments, the remedy obtained through state

enforcement included not only a monetary penalty, but also important injunctive relief requiring the businesses to adopt measures to better secure customer information.

As this Committee considers changes to federal law, I urge the Committee to do so mindful of the robust state laws and enforcement activity already in place. From California's expertise and enforcement experience, two principles are critically important for federal legislation:

First, any changes to the federal regime should not preempt California's strong data security, breach notification, or other information security laws. Preemption provisions included in any federal legislation should be limited and carefully tailored to preempt only less protective state laws. It is appropriate for Congress to provide a floor for data security standards, but states must be able to continue to require more robust protection for the privacy interests of our residents. The federal regime must also continue to allow states to move swiftly to innovate, adopting stronger and modernized data security laws, given the rapid evolution of technology and threats to data security and consumer privacy.

Second, any federal legislation should not undermine the enforcement role of the state attorneys general. State enforcement of data security and breach notification laws is critical to successfully holding businesses accountable for these breaches, obtaining appropriate penalties and injunctive relief, and protecting our residents. California and our sister states can tackle large, nationwide challenges, such as the Equifax breach, and smaller, localized breaches such as when Kaiser Foundation Health Plan allowed an unencrypted USB drive with employee Social Security numbers to wind up for resale at a thrift store. States are able to be responsive to the particular threats facing our communities, nimble in our enforcement work, and close to the ground in our engagement with residents grappling with the consequence of breach. As Americans across the country become more vulnerable to data security failures, we cannot afford to take any cops off the beat.

Attorney General Becerra is committed to vigorously using legal tools to protect the privacy interests of Californians and to collaborating with our state and federal partners to improve data security, breach notification, and remediation in the event of a breach across the country. Any changes to the federal regulatory regime covering data security and breach notification must not weaken protections for Californians. Federal law should be a floor, not a ceiling, working in concert with state law and enabling the ongoing innovation and vigorous protection offered by the states.

⁶ *Attorney General Becerra Announces \$3.5M Settlement with Lenovo for Preinstalling Software that Compromised Security of its Computers*, available at <https://oag.ca.gov/news/press-releases/attorney-general-becerra-announces-35m-settlement-lenovo-preinstalling-software>.