PROTECTING CRITICAL INFRASTRUCTURE: HOW THE FINANCIAL SECTOR ADDRESSES CYBER THREATS

HEARING

BEFORE THE

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

OF THE

COMMITTEE ON FINANCIAL SERVICES

U.S. HOUSE OF REPRESENTATIVES

ONE HUNDRED FOURTEENTH CONGRESS

FIRST SESSION

MAY 19, 2015

Printed for the use of the Committee on Financial Services

Serial No. 114–26

U.S. GOVERNMENT PUBLISHING OFFICE

95–070 PDF WASHINGTON : 2015

For sale by the Superintendent of Documents, U.S. Government Publishing Office
Internet: bookstore.gpo.gov Phone: toll free (866) 512–1800; DC area (202) 512–1800
Fax: (202) 512–2104 Mail: Stop IDCC, Washington, DC 20402–0001

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
SCOTT GARRETT, New Jersey
RANDY NEUGEBAUER, Texas
STEVAN PEARCE, New Mexico
BILL POSEY, Florida
MICHAEL G. FITZPATRICK, Pennsylvania
LYNN A. WESTMORELAND, Georgia
BLAINE LUETKEMEYER, Missouri
BILL HUIZENGA, Michigan
SEAN P. DUFFY, Wisconsin
ROBERT HURT, Virginia
STEVE STIVERS, Ohio
STEPHEN LEE FINCHER, Tennessee
MARLIN A. STUTZMAN, Indiana
MICK MULVANEY, South Carolina
RANDY HULTGREN, Illinois
DENNIS A. ROSS, Florida
ROBERT PITTENGER, North Carolina
ANN WAGNER, Missouri
ANDY BARR, Kentucky
KEITH J. ROTHFUS, Pennsylvania
LUKE MESSER, Indiana
DAVID SCHWEIKERT, Arizona
FRANK GUINTA, New Hampshire
SCOTT TIPTON, Colorado
ROGER WILLIAMS, Texas
BRUCE POLIQUIN, Maine
MIA LOVE, Utah
FRENCH HILL, Arkansas

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
RUBÉN HINOJOSA, Texas
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
JOHN C. CARNEY, JR., Delaware
TERRI A. SEWELL, Alabama
BILL FOSTER, Illinois
DANIEL T. KILDEE, Michigan
PATRICK MURPHY, Florida
JOHN K. DELANEY, Maryland
KYRSTEN SINEMA, Arizona
JOYCE BEATTY, Ohio
DENNY HECK, Washington
JUAN VARGAS, California

SHANNON MCGAHN, *Staff Director*
JAMES H. CLINGER, *Chief Counsel*

SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

RANDY NEUGEBAUER, Texas, *Chairman*

STEVAN PEARCE, New Mexico, *Vice Chairman*
FRANK D. LUCAS, Oklahoma
BILL POSEY, Florida
MICHAEL G. FITZPATRICK, Pennsylvania
LYNN A. WESTMORELAND, Georgia
BLAINE LUETKEMEYER, Missouri
MARLIN A. STUTZMAN, Indiana
MICK MULVANEY, South Carolina
ROBERT PITTENGER, North Carolina
ANDY BARR, Kentucky
KEITH J. ROTHFUS, Pennsylvania
FRANK GUINTA, New Hampshire
SCOTT TIPTON, Colorado
ROGER WILLIAMS, Texas
MIA LOVE, Utah

WM. LACY CLAY, Missouri, *Ranking Member*
GREGORY W. MEEKS, New York
RUBÉN HINOJOSA, Texas
DAVID SCOTT, Georgia
CAROLYN B. MALONEY, New York
NYDIA M. VELÁZQUEZ, New York
BRAD SHERMAN, California
STEPHEN F. LYNCH, Massachusetts
MICHAEL E. CAPUANO, Massachusetts
JOHN K. DELANEY, Maryland
DENNY HECK, Washington
KYRSTEN SINEMA, Arizona
JUAN VARGAS, California

CONTENTS

PROTECTING CRITICAL INFRASTRUCTURE: HOW THE FINANCIAL SECTOR ADDRESSES CYBER THREATS

Tuesday, May 19, 2015

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 12:59 p.m., in room 2175, Rayburn House Office Building, Hon. Randy Neugebauer [chairman of the subcommittee] presiding.

Members present: Representatives Neugebauer, Pearce, Lucas, Posey, Fitzpatrick, Westmoreland, Luetkemeyer, Stutzman, Mulvaney, Pittenger, Barr, Guinta, Tipton, Williams, Love; Clay, Hinojosa, Velazquez, Lynch, Heck, Sinema, and Vargas.

Chairman NEUGEBAUER. The Subcommittee on Financial Institutions and Consumer Credit will come to order. Without objection, the Chair is authorized to declare a recess of the subcommittee at any time.

Today's hearing is entitled, "Protecting Critical Infrastructure: How the Financial Sector Addresses Cyber Threats."

Before I begin, I would like to thank our witnesses for being here today and for traveling all the way over to 2175. We had a little preview of our new digs, but there is a thing in construction called a "punch list," and I think we had to remove ourselves for a week or so, so they could work on a punch list over there. But we hope to be back in there soon.

As a little bit of housekeeping, I am sure that the majority leader forgot I was having a hearing this afternoon and has scheduled votes sometime here in the next few minutes. And I am sure that was an oversight on his part. But nonetheless, we will have Members who have to go vote. We are going to take care of that little constitutional duty.

I will just remind everyone that the Chair is authorized to call a recess at any time, and so the Members can vote. So I think what we are going to try to do here is we are going to have opening statements and we are going to keep going until they ring the bell. We will ask Members to quickly go over and vote, and we will come back and resume the hearing. After that, we should be good to go for the rest of the hearing.

I am now going to recognize myself for 5 minutes to give an opening statement.

The financial services sector is one of the most complex and critical sectors of the U.S. economy.

Financial sector participants hold deposits for consumers; ensure the consistent flow of capital through our capital markets; provide loans for small businesses; support large, internationally active corporations; and operate some of the most sophisticated payment systems on the globe.

Literally trillions of dollars flow through the financial sector each and every single day. Given its position of critical importance, the financial services sector has become a top target for cyber attacks.

Today and every day this year, there will be 117,334 cyber incidents against the U.S. economy, according to a PricewaterhouseCoopers study.

A recent Depository Trust & Clearing Corporation study highlighted cybersecurity as the number one issue of concern for financial institutions. This top position is held over risks such as overregulation and geopolitical risks.

Last week, SEC Chair Mary Jo White noted that cyber attacks are the "biggest systemic risk" facing the United States of America. And Treasury Secretary Jack Lew noted that cybersecurity is one of those issues that keeps him up at night.

Given the importance of this threat, the financial services sector has responded well. The sector has been a leader in setting up an information-sharing framework and has been an active and constructive participant in working with U.S. regulatory agencies and law enforcement. And further, the sector's investment in cybersecurity infrastructure and engagement by senior management has been crucial to preventing future attacks.

However, we should all remember that there is no single institution or system that is 100 percent protected from cyber attacks. The sector faces threats posed by a growing array of cyber criminals, national and state actors, and terrorist organizations. Each has tremendous financial and political incentive to continue looking for weak spots, and to cause sector disruption.

Today's hearing is important for Members to gain a better understanding of some of the top cyber issues facing the financial services sector.

First, we must better understand the nature of cyber threats. Where are threats coming from? What do they look like? And how are we working with global partners?

Second, information-sharing and liability protection are crucial elements to a cyber response framework. We should explore how public-private partnerships help facilitate comprehensive responses to cyber threats, and if there are areas where we should be and can be improving.

Third, contingency preparation is critical to being able to provide continuity in the sector in the wake of a cyber attack. We should better understand the steps the financial services sector is taking to plan for attacks, train employees, and test its system.

Cybersecurity is a shared responsibility. It is a shared responsibility among financial institutions. It is a shared responsibility between the public sector and the government. It is a shared responsibility between the United States and our global allies.

And finally, being thoughtful leaders on this issue is a shared responsibility for members of this committee. I would like to thank my Democratic colleagues for taking this issue so seriously and contributing to a very constructive dialogue.

I would now like to recognize the ranking member of the subcommittee, Mr. Clay, for 3 minutes.

Mr. CLAY. Thank you, Mr. Chairman, and thank you to each of today's witnesses for your testimony. I welcome today's testimony from our panel of practitioners and content area experts. And I view this afternoon's hearing as an important opportunity to shed some light on the financial services industry's ability to effectively monitor, detect, and respond to cyber attacks.

Cyber criminals, state-sponsored and affiliated hackers, and politically-motivated "hacktivists" have all targeted the financial services industry. And their tactics have continued to evolve and expand in frequency, scale, sophistication, and severity.

To that end, the financial services industry's response, monitoring, and information-sharing infrastructure, as well as the response capabilities of the relevant Federal regulators, must reflect the dynamic nature of cyber threats.

Mr. Chairman, I firmly believe that cybersecurity is one of a few issues where our committee can truly work in a bipartisan fashion to ensure that our regulators and regulated entities have the necessary resources and support to defend against cyber attacks. I look forward to each witnesses' testimony, and I yield back the balance of my time.

Chairman NEUGEBAUER. The Chair now recognizes the gentlewoman from Arizona for 2 minutes.

Ms. SINEMA. Thank you, Mr. Chairman. When hackers stole the credit card information of Susan, one of my constituents from Chandler, Arizona, she initially didn't notice an unauthorized $10 donation to a small charity, but the next month she did notice the several hundred dollars in police uniforms that a man in London had purchased using her card, and that is when she called the FBI.

Unfortunately, Susan's story is all too common. Last year alone, according to Verizon's 2015 Data Breach Investigations report, there were more than 79,000 security incidents reported and more than 2,000 confirmed data breaches. These breaches have exposed the personally identifiable information, as well as sensitive financial information, of millions of consumers.

Securing the financial services sector requires us to continue to strengthen security practices and information-sharing infrastructures.

Educating consumers and financial sector participants is also crucial if these efforts are to be successful.

The evolving nature of cyber threats calls for a vigorous and dynamic response. I look forward to hearing more from our witnesses today about how industry is developing safety protocols that keep pace with technological innovation, and how educating consumers and financial sector participants will help better protect consumers like my constituent, Susan.

Thank you, Mr. Chairman. I yield back my time.

Chairman NEUGEBAUER. I thank the gentlewoman.

We will now turn to our witnesses. Today we welcome the testimony of the Honorable Kenneth E. Bentsen Jr., president and CEO of SIFMA; Mr. Gregory T. Garcia, executive director of the Financial Services Sector Coordinating Council; Mr. Robert S. Nichols, president and CEO of the Financial Services Forum; Mr. Russell Fitzgibbons, executive vice president and chief risk officer for The Clearing House Payments Company; and Mr. Jason Healey, senior research scholar at the School of International and Public Affairs, Columbia University, and senior fellow at the Atlantic Council.

You will each be recognized for 5 minutes to give a summary of your testimony, and without objection, your complete written statements will be made a part of the record. We would ask you to limit your remarks to 5 minutes.

Mr. Bentsen, you are now recognized for 5 minutes.

STATEMENT OF THE HONORABLE KENNETH E. BENTSEN, JR., PRESIDENT AND CHIEF EXECUTIVE OFFICER, THE SECURITIES INDUSTRY AND FINANCIAL MARKETS ASSOCIATION (SIFMA)

Mr. BENTSEN. Thank you, Chairman Neugebauer, Ranking Member Clay, and members of the subcommittee for allowing me the opportunity to testify on this critically important topic.

A large-scale cyber attack resulting in the destruction of books and records and disruption of our capital markets is among the most significant and systemic threats facing our economy today, so it is appropriate that so much time and energy is being focused on developing public-private partnerships and identifying solutions to mitigate that risk.

The financial services sector has invested huge sums of capital into their cyber attack deterrence programs over the years, enhancing their efforts to match the growing threat.

As policymakers and the industry focus on addressing the causes of the last financial crisis, it is equally, if not more important that we focus on the future risks, and cyber crime is the greatest.

Some 18 months ago, SIFMA's members commenced the five-part multiyear effort to address cybersecurity threats and related risks to broker-dealers and asset managers. Emanating from our previous work as part of the industry's business continuity planning, and in response to the 2014 NIST framework, the goal of these five initiatives is to better identify the vulnerabilities to our sector and to prepare individual firms of all sizes and the broader sector to defend themselves and our clients, thereby enhancing protection for the millions of Americans who access these markets every day.

My written testimony goes into much more detail on these five initiatives, but I would like to touch on just a few.

SIFMA recently published its principles for effective cybersecurity regulatory guidance and called for regulations to be harmonized across agencies for greater effectiveness. These principles build upon the highly valuable NIST framework, an initiative which we contributed much time and energy to, and after its release have sought out opportunities to promote its use within the sector by mapping existing compliance requirements so firms can see where they could not only enhance risk management, but compliance as well.

The industry also looks to the government to help identify uniform standards, promote accountability across the entire critical infrastructure, and provide access to the essential information. SIFMA urges policymakers to consider how best to incorporate the principles into the respective regulatory initiatives. Importantly, regulators should coordinate their efforts to ensure harmonization.

SIFMA assembled a working group to develop a diagnostic on the U.S. equity and treasury markets to determine the sector's resiliency during the attack. After mapping process flows within these markets, a workshop was held during which a set of 10 diverse cyber risk scenarios were applied to the markets, and a number of potential vulnerabilities were identified.

These results are being addressed via a number of public and private internal working groups. As a result of this exercise, we have undertaken efforts with the accounting industry and the American Institute of CPAs (AICPA) to develop a third-party vendor risk audit standard, referred to as SOC 2, that should provide increased transparency and accountability with third party vendors.

Building off of the lessons learned from the SIFMA-sponsored cyber exercise "Quantum Dawn 2" in 2013, and from our experience in Superstorm Sandy, SIFMA continues to revise the industry's playbook for responding to a cyber attack which could result in market closures. On a continuing basis, we are working with stakeholders including exchanges, clearinghouses, and regulators to ensure the current state of readiness.

Our dialogue with the FSSCC and with our partners in government has evolved into a joint exercise program of quarterly tabletop exercises and other large-scale simulations to test industry preparedness and response. Additionally, we have made substantial progress in developing an improved process to request technical assistance from the Federal Government in the midst of a cyber attack. This pre-positioning will help reduce the time it takes to engage the relevant civilian and law enforcement agencies to assist firms.

SIFMA and its member firms have spent considerable time and energy to improve cyber threat information-sharing both within our sector and with our government partners. And at a high level, there has been increased collaboration and communication between the government and the financial services industry.

Importantly, we are endeavoring to continue this collaboration on a regular basis, again to ensure a current state of readiness. There is room for further improvement. However, I would like to flag three recommendations for this committee's consideration.

First, our industry needs clarity on which government authority is responsible for each specific aspect of cybersecurity.

Second, the financial services sector would benefit from higher quality and more frequent classified briefings.

And third, we need Congress to get a cybersecurity information-sharing bill to the President before the next crisis, not after.

Neither the industry nor the government can prevent or prepare for cyber threats on their own. SIFMA has brought together experts from across the public and private sectors to better understand the risks involved in a cyber attack and to develop best prac-

tices to be prepared to thwart an attack, but to be effective, we must work closely with the Federal Government to strengthen our partnership, and protect our economy and the millions of Americans who place their confidence and trust in the financial markets each and every day.

Thank you.

[The prepared statement of Mr. Bentsen can be found on page 40 of the appendix.]

Chairman NEUGEBAUER. I thank the gentleman.

Now, Mr. Garcia, you are recognized for 5 minutes.

STATEMENT OF GREGORY T. GARCIA, EXECUTIVE DIRECTOR, FINANCIAL SERVICES SECTOR COORDINATING COUNCIL (FSSCC)

Mr. GARCIA. Thank you, Chairman Neugebauer, Ranking Member Clay, and members of the subcommittee for the opportunity to testify today.

I am the executive director of the Financial Services Sector Coordinating Council, or FSSCC, which was established in 2002. FSSCC involves 66 of the largest financial firms and their industry associations. I am also pleased to be able to share the witness table today with the FSSCC chairman, Mr. Russell Fitzgibbons.

Today I will discuss how we are organized under regulatory and partnership frameworks to manage the cyber risks and threats that are faced by the financial sector.

The financial sector operates over a network of information and communications technology platforms, making cybersecurity of paramount importance to the sector. A successful cybersecurity or physical attack on these systems could have significant impacts on the global economy and the Nation.

For example, malicious cyber actors vary considerably in terms of motivation and capability, from nation-states conducting corporate espionage to sophisticated cyber criminal groups stealing money, to "hacktivists" intent on making political statements. Many cybersecurity incidents, regardless of their original motive, have the potential to disrupt critical systems, even inadvertently.

Thus, the FSSCC's mission is to strengthen the financial sector's resilience against attacks and other threats. We work with the Treasury Department, law enforcement, the Department of Homeland Security, the intelligence community, and regulators toward four main objectives.

First, identify threats through robust information-sharing.

Second, promote protection and preparedness through best practices.

Third, coordinate incident response through joint exercises.

And fourth, consider how the policy environment can promote the above activities.

In practice, these objectives have yielded numerous accomplishments for the benefit of the sector and the economy over the past 10 years.

For example, just to list a few recent examples, we are improving information-sharing content and procedures between government and the sector. We have developed and we maintain an all-hazards crisis response playbook and a cyber response coordination guide

that lead our incident responders and our executive decision-makers through decision and action procedures during an incident.

Also, we are conducting joint exercises affecting different segments of the financial system. As Mr. Bentsen alluded to, we maintain a physical presence in the Department of Homeland Security's National Cybersecurity and Communications Integration Center, or NCCIC. This serves as a hub for sharing information related to cybersecurity and communications incidents across sectors.

Our representative there is cleared at the Top Secret/SCI level. Relatedly, we have worked closely with government partners to obtain security clearances for key financial services sector personnel. These clearances have been used to brief the sector on new information security threats and have permitted the exchange of timely and actionable information. We develop best practices involving third-party risks, supply chain, and cyber insurance strategies, among many others.

To go on, we have developed research and development priorities to improve the tools for protection resilience. We are engaging with other critical sectors and international partners to understand and leverage our interdependencies such as communications and electricity.

We have created a financial sector-owned, operated, and governed .bank and .insurance top-level Internet domains. When the Internet-governing authority expanded the number of the so-called top-level domains beyond .com, .gov, .org, .edu, et cetera, they expanded them to hundreds of different names, but we established the .bank and .insurance domains on our own to ensure that we have security standards to protect our system from fraud and cyber attack. This includes imposing eligibility requirements, verification, name selection standards, and other security-focused technical requirements.

Our operational arm, the Financial Services Information Sharing and Analysis Center, or FS-ISAC, has developed a technical tool called Soltra Edge that automates threat sharing and analysis and speeds the time to decision and mitigation from days to hours and minutes.

Finally, a word about regulation. Mr. Chairman, the financial sector is often credited for having developed a mature cybersecurity risk management posture. This is due in part to the fact that financial services is a heavily regulated industry, but it is also because our business models, consumer confidence, and the stability of the financial system are dependent upon a secure and resilient infrastructure. We really can't afford to be complacent.

The financial sector supports the need for regulatory guidance on effective standards of practice for cyber risk management, but as the regulatory agencies are independent, there is not sufficient coordination among them in our experience. One institution may face multiple and differing sets of examination questions about the same security controls depending on which regulator is doing the assessment.

We would urge more uniformity among the regulatory agencies in their examination procedures. This process could be more efficient so that financial firms can focus more on securing our infrastructure and less on answering multiple questionnaires in dif-

ferent ways. We need to ensure we are all aligned with unity of effort toward a common objective: financial services security and resiliency.

Mr. Chairman, that concludes my testimony. I will be happy to answer any questions.

[The prepared statement of Mr. Garcia can be found on page 54 of the appendix.]

Chairman NEUGEBAUER. I thank the gentleman.

Mr. Nichols, you are now recognized for 5 minutes.

STATEMENT OF ROBERT S. NICHOLS, PRESIDENT AND CHIEF EXECUTIVE OFFICER, FINANCIAL SERVICES FORUM

Mr. NICHOLS. Thank you, Mr. Chairman, Ranking Member Clay, and members of the subcommittee for the opportunity to participate in today's hearing on the threat posed by cyber attacks to our financial system.

As you mentioned, I am here as the CEO of the Financial Services Forum, which is a financial and economic policy organization comprised of the CEOs of 18 of the largest and most diversified financial institutions doing business here in the United States.

Your hearing is both enormously important and remarkably timely. In recent years, cyber attacks have grown rapidly, both in number and level of sophistication. According to Symantec Corporation, a leading information and Internet security firm, cyber attacks around the world have soared 91 percent in 2013 alone.

Just last week, the Depository Trust & Clearing Corporation, a New York-based securities settlement and clearing firm, released its Systemic Risk Barometer for the first quarter of 2015, based on a survey of financial market participants. Asked to identify the top risks to the financial system, respondents cited cyber attacks. Indeed, nearly half of the respondents, 46 percent, cited cybersecurity as their top concern, with respondents specifically noting the growth in the frequency and sophistication of cyber attacks.

Effectively defending against the mounting threat of cyber attacks requires resources, technical sophistication, and cooperation among financial institutions and between the financial industry, other critical infrastructure sectors, and the relevant government agencies. Large financial institutions are working hard to deliver every day on each of those critical fronts.

With regard to resources and technical expertise, large financial institutions remain at the cutting edge of cyber protection and are regarded by most experts—both in the public sector and the private sector—as having developed and deployed some of the most sophisticated and effective defenses against cyber attacks in the corporate world.

With regard to industry cooperation and coordination, cybersecurity in the financial sector is a team effort—because it has to be. To be successful, the industry must invest in, and operate within, a single unified cybersecurity culture.

In particular, large financial institutions are investing in evermore robust and automated systems of threat analysis and sharing. Automated threat analysis enables the quick and reliable detection and diagnosis of threats. And automated sharing enables the swift dissemination of clear and precise threat information across the fi-

nancial system. In a very real sense, large financial institutions serve, as one could say, as the forward guard of America's cyber defenses.

Cooperation between industry and government is vital if the battle against mounting cyber threats is to be won. To encourage better cyber threat information-sharing within the financial sector and between industry and government, legislation providing sensible "Good Samaritan" protections is needed.

Such legislation should facilitate real-time cyber threat information-sharing to enable financial institutions and government to act quickly; provide liability protection for good faith cyber threat information-sharing; provide targeted protections from public disclosures, such as exemptions from certain Freedom of Information Act requests; facilitate appropriate declassification of pertinent government-generated cyber threat information and expedite issuance of clearances to selected and approved industry executives; and lastly, include appropriate levels of privacy protections.

With these needs in mind, the bill passed by the House on April 22nd, which, of course, you supported, Mr. Chairman, is a major and important step forward, and will greatly facilitate industry's cooperation with government. We hope the Senate will soon take up its information-sharing proposal to continue progress on this important issue. We would urge swift movement and passage on that important legislation.

On behalf of the Forum and its members, I commend you for drawing attention to this issue and this effort. We look forward to working with you in the days ahead.

Thank you, Mr. Chairman.

[The prepared statement of Mr. Nichols can be found on page 68 of the appendix.]

Chairman NEUGEBAUER. I thank the gentleman.

Mr. Fitzgibbons, you are now recognized for 5 minutes.

STATEMENT OF RUSSELL FITZGIBBONS, EXECUTIVE VICE PRESIDENT AND CHIEF RISK OFFICER, THE CLEARING HOUSE PAYMENTS COMPANY L.L.C.

Mr. FITZGIBBONS. Thank you, Chairman Neugebauer, Ranking Member Clay, and members of the subcommittee. My name is Russ Fitzgibbons, and I am the executive vice president and chief risk officer of The Clearing House Payments Company.

As the chief risk officer, I am responsible for enterprise risk management, information security, and business continuity. I also serve, as referenced by Mr. Garcia, as the current Chair of the Financial Services Sector Coordinating Council. I appreciate the opportunity to appear before you today to discuss issues that are critical to all Americans—the protection of our payment systems against cyber threats.

The Clearing House is the Nation's oldest banking association and payments company, founded in 1853, and currently owned by 26 banks. We provide payment, clearing, and settlement services to our owner banks and other financial institutions, clearing and settling nearly $2 trillion daily. The Clearing House also engages in payments technology and payments systems security advocacy.

The Clearing House operates the Clearing House Interbank Payments System, commonly referred to as CHIPS, and we are a leading participant in the Automated Clearing House, referred to as ACH, network. We are the only private-sector ACH operator in the country, processing approximately 50 percent of all commercial ACH volume in the United States through our networks.

CHIPS is the largest private-sector US-dollar funds transfer system in the world, clearing and settling an average of $1.5 trillion in payments—both domestic and cross-border—daily.

Because of the volume and importance of the financial transactions enabled by The Clearing House's systems, robust protection of these systems from cyber threats is essential. Those threats have become more frequent and more sophisticated in recent years. The criminal organizations and other groups launching these threats are constantly innovating, and we need to be at least as agile as they are in defending ourselves.

I would like to discuss some of the ways in which The Clearing House works both on its own and frequently in collaboration with other financial services firms to defend itself and its institutional customers against cyber threats.

First, like others in our sector, The Clearing House is subject to special legal and regulatory requirements such as those promulgated by the Federal financial regulatory agencies of the Federal Financial Institutions Examination Council, the FFIEC. The Clearing House's data security practices are subject to regular examination and supervision through the FFIEC's Multi-Regional Data Processing Servicers Program, referenced as MDPS.

Second, we are constantly innovating. One example of innovation for improved cyber defense is a new platform of The Clearing House which replaces account numbers with randomly generated temporary numbers during processing. With Secure Token Exchange, the customer's actual account information remains behind bank firewalls while preserving the current customer experience.

Third, we engage in training and exercises through simulations that put our cyber defense processes to the test and identify areas for improvement.

Finally, we engage in extensive information-sharing by actively engaging with the FS-ISAC, its member organizations, and our government partners. Truly effective cybersecurity will also require increased efforts by the Federal Government to defend the financial sector against threats often originating overseas, and above all, more effective collaboration between the private sector and the government.

My written statement details some of the additional components of our information-sharing efforts. However, I would like to mention a couple of them.

Through FS-ISAC and the Depository Trust & Clearing Corporation, the sector recently deployed a more effective platform for real-time automated sharing of cyber threat information called Soltra Edge. Utilization and integration of Soltra Edge across the sector's infrastructure is expected to scale significantly over the next few years.

We also coordinate closely with the National Infrastructure Coordinating Center, the Department of Homeland Security's Oper-

ation Center that maintains awareness of critical infrastructure for the Federal Government. We participate actively in the Financial Services Sector Coordinating Council, and we also work closely with the Treasury Department's office for critical infrastructure, protection and compliance, and its cyber intelligence group.

While the financial services sector has made considerable strides in its sharing with the sector and with our government partners, there are still areas for improvement. Companies in the financial sector share information quite extensively with the government. We have lots of opportunity to improve our ability to support our cyber first responders, defend critical infrastructure, and protect our stakeholders.

To that end, the Administration has issued two Executive Orders designed to improve sharing from the government to the private sector, and there have been resulting improvements. But we think more work could be done with the analysis of threat information, and government agencies need to continue to increase prioritization and allocation of resources for declassification of information that pertains to network defense.

I would also add that we believe Congress has an important role to play in promoting greater and more effective cybersecurity information-sharing. We support two bills that have passed the House, and we support the information-sharing legislation that is moving through the Senate. And we would urge you to move as quickly as possible to get those bills to the President's desk.

Thank you again for the opportunity to testify, and I look forward to your questions.

[The prepared statement of Mr. Fitzgibbons can be found on page 47 of the appendix.]

Chairman NEUGEBAUER. I thank the gentleman. And Mr. Healey, you are recognized for 5 minutes.

STATEMENT OF JASON HEALEY, SENIOR FELLOW, THE ATLANTIC COUNCIL

Mr. HEALEY. Chairman Neugebauer, Ranking Member Clay, and distinguished members of the subcommittee, thank you for the honor of testifying today.

Over the past nearly 20 years, I have been involved in cyber operations and policy in the military and intelligence community, the White House, and the finance sector. Now, with Columbia University's SIPA and the Atlantic Council think tank, I may be less involved in the day-to-day cyber tumult than my colleagues, but with a bit more freedom to analyze what might be next. Therefore, in the interest of time, I will agree with the strength of the sector that my colleagues have already mentioned in order to look ahead.

Last year we published the first history of cyber conflict of how states have really, over the past 25 years, fought in cyberspace. One of the key lessons is that it may be easy to disrupt a target using the Internet but it is far more difficult to keep it down over time in the face of determined defenses. And as we saw after the attacks of September 11th, the finance sector can be extremely determined.

Therefore, looking forward, I believe the committee need not be overly concerned about a James Bond-style large-scale disruptive

attack taking down the sector. This should not mean that we should rest on our successes to date.

In fact, I am deeply worried that the finance sector will get caught up in what I believe is the Internet's most dangerous moment. If nuclear talks with Iran collapsed, there might be a rapid spike in truly disruptive attacks by a dangerous cyber adversary who has already struck at U.S. financial targets. Worse, President Putin of Russia may likewise feel that with his own economic back against the wall, it is time to retaliate with some just deniable enough little green bytes. Facing potentially existential regime threats, Iran and Russia may see little downside to digitally lashing out against a global financial system in which they have few remaining stakes.

As an example of what we might expect, while a next generation Sony-style attack would not take down the sector as a whole, it might seriously disrupt a systemically important financial institution so that it could not clear or settle within—by the end of the day. These dangers require immediate contingency planning and can—including exercises such as those my colleagues have talked about within the sector and with the regulators and other Federal and international partners.

On the government side, the Executive Branch could do a better job of leading from the front and sharing protection and restraint.

The government berates companies to share information, but despite recent gains, it keeps too much information classified or stuck behind bureaucratic barriers. It may need some added push from committees like yours, which oversees the sectors which so desperately need that stuck information.

Likewise, as someone who has proudly worked in both the public and private sectors, it is frustrating to hear bureaucrats or even directors of NSA complain that companies miss standards even in the face of their own Federal Information Security Management Act (FISMA) scores. And even though it should be in the long-term interest of the United States that financial infrastructures should be off-limits to cyber attacks, the Department of Defense has not yet made clear statements to create that norm.

In conclusion, this subcommittee might also usefully push the Executive Branch to think of a broader set of possible responses to give the finance sector more staying power in the event of a sustained conflict such as against Russia or China.

When I was working finance sector-wide events with the FS-ISAC, our responses could have been far more successful not with DOD suppressing fire or cyber ninjas, but with solid officers and NCOs ready to roll up their sleeves to help corral the countless details of a major response. In the face of nation-state cyber threats, we would not want the sector to stumble simply for the lack of a few MOUs in place beforehand for more flexible partnerships.

And if you remember, the FS-ISAC would likely never have been as strong as it is today, if it had not been recapitalized 12 years ago by a grant from Treasury, with the proviso that it would provide service to all regulated American financial institutions, not just those who paid a membership fee. It may be the time for additional innovation using grants, perhaps not directly to the sector

anymore, but to the countless other non-stake groups who help defend this Nation's critical infrastructure.

Thank you for your time.

[The prepared statement of Mr. Healey can be found on page 62 of the appendix.]

Chairman NEUGEBAUER. I thank the gentleman. The Chair now recognizes himself for 5 minutes for questions.

Mr. Garcia and Mr. Fitzgibbons, in your testimony you talked about Soltra Edge, and I was kind of intrigued by that process. Evidently, that is an electronic detection and notification software, I assume. I am interested in how that database is updated, and then what is the distribution once a detection is made? Obviously, it is meant to be an information-sharing tool, so what is the dissemination process on that?

Mr. FITZGIBBONS. Sure. So I will start, great. The benefit of Soltra Edge actually recognizes the fact that while it is widely accepted that information-sharing is the right thing to do, sharing that information when done effectively creates a ton of information—extraordinary amounts of information. And what was recognized is that the recipients, through the FS-ISAC, for example, who would get this—these threat indicators, it was a lot of work to try and get it into their systems and so forth.

We recognized that to really be effective, we needed to automate that stream, and we needed to create a machine-readable language. We needed to create standards by which that information would actually transit from the FS-ISAC onto or through the Soltra system onto the various firms that participate.

So what actually happens is that all the members who have come across threat indicators will put them into the system using the appropriate standards and so forth. And then by joining that system and participating in it, you will be the recipient of that information so you can protect yourselves using information that the whole community has actually uncovered about threats that are actually emanating. And then you can update your detection systems automatically, and that is really the benefit of it all, to take this opportunity to take something that is created by many and then share it out to everyone else quickly and effectively in a machine-readable form that can be updated to systems.

Chairman NEUGEBAUER. Mr. Garcia, do you want to elaborate on that?

Mr. GARCIA. Yes. Mr. Fitzgibbons is exactly right. It is a fact that machine-to-machine information-sharing enables faster response times and better, more uniform analysis of the threats, making sense of what we are seeing. And I think we credit that a lot to a standard developed by the Department of Homeland Security, they are called STIX and TAXII. I won't go into the acronym. But one of them describes a common nomenclature, a common language, a dictionary for how we refer to threats and all of the various characteristics of those threats. And the other one is a common communications platform so that everybody can use this. So this is taxpayer dollars well spent.

It is a standard and open specification that is available to all sectors. And the financial sector has overlaid on top of those standards

a software program that enables us to share among ourselves, and if we so choose, with other sectors as well.

Chairman NEUGEBAUER. Thank you.

Mr. Bentsen, I think you mentioned in your testimony that over the last several years, you have held cyber attack simulations to kind of, I guess, prepare for what if, and how to respond. Can you tell us some of the benefits that have come out of hosting those simulations?

Mr. BENTSEN. Yes, Mr. Chairman, a couple of things. Over the years, we have run a couple of simulations, Quantum Dawn 1, and Quantum Dawn 2, which was most recently in 2013. We will be doing a Quantum Dawn 3 in the third quarter of this year.

The Quantum Dawn 2 exercise, and then some subsequent tabletop exercises that we have done with our government partners as well as our partners at this table, allow us to iteratively grow our capabilities to respond to identify gaps in whether it is information-sharing, coordination, whether we have the right parties involved. In the case of Quantum Dawn 2, which was a simulated attack on the U.S. equity markets and multi-pronged simulated attack on the U.S. equity markets, the outtakes from that were that we needed more engagement from our exchange partners and that we needed a better coordination mechanism going into a situation recovery that was talked about here as well.

So our view is that these exercises are good not just on a one-off basis but on an ongoing basis. And one of the things that we have talked with our government partners about is to continue both these large simulations and tabletop exercises on a regular basis so we maintain a state of readiness and we don't atrophy in the process.

Chairman NEUGEBAUER. And do you generate a deliverable then that is shared across the industry and with all the participants—

Mr. BENTSEN. What we did in the case of Quantum Dawn 2, is we used that as well as our experience coming out of Superstorm Sandy, which did result in a closing of the equity and fixed income markets to improve our playbook with the exchanges with the regulators, with the industry partners, and those involved in it.

Likewise in the tabletops, we are trying to come out with deliverables both for the industry and for the government.

Chairman NEUGEBAUER. I thank you.

And now the gentleman from Missouri, the ranking member of the subcommittee, Mr. Clay, is recognized—

Mr. CLAY. Thank you so much, Mr. Chairman.

Chairman NEUGEBAUER. —for 5 minutes.

Mr. CLAY. Let me start with Mr. Healey. Given the level of sophistication of cyber attacks from China, in particular, is it reasonable to expect that financial institutions will be successful in stopping them?

Mr. HEALEY. We have been learning over time that a determined offense will almost always get through. This is not a recent trend; we have seen quotes that go back to the 1970's that essentially say the bad guys are going to get through if they want to. So the best, I think, any company, any organization can do is to not just try to keep them out, but to do what the financial—I think it has been

pretty good at, at least at the main institutions, is presumption of breach.

Assume that there is already a heist going on, that you have a sophisticated set of diamond thieves who are already inside the bank, and then how do you find those sophisticated diamond thieves when they are inside? I suspect JPMorgan Chase would not have discovered an intrusion of they hadn't been using this presumption of breach.

But this is still difficult. It is tough even for the big institutions to do, so I am worried about how the small and medium-sized financial institutions are going to try to catch up.

Mr. CLAY. Anyone else? Mr. Fitzgibbons?

Mr. FITZGIBBONS. One of the things I would mention—I agree very much with Mr. Healey, but one of the things that is really a benefit of—gets to the small and medium institutions of an institution such as FS-ISAC that it does take advantage of the resources, the experiences, and so forth of a firm such as, I heard reference to JPMorgan.

When you go into the ISAC, that is where those threat indicators are shared. And then when you go into some of the other forms where tactics and techniques are discussed, as well so using a form such as the ISAC, actually allows us to take those lessons learned and those resources available at some of the larger firms and get it out to the smaller and the medium banks and so forth.

And that is why the partnership with a membership in the ISAC is so important and why we have seen it growing as well; everybody is trying to avail themselves of that.

Mr. CLAY. Mr. Bentsen?

Mr. BENTSEN. Mr. Clay, I would add two things to that. First, following up on Russ' comments, expanding the membership of the ISAC is critically important. And what we and others have tried to do is one, to get all of our members to participate in it, to encourage our regulators—FINRA, SEC, and others—to encourage to the extent they can that all of their regulated entities are participating in the ISAC.

Two, to develop standards across the sector that aren't just for the larger institutions who may have more capabilities, but for all members because they are all linked together. They are all trading together.

The other thing—the point I would make is, I don't think we can stand up here and say that we can create an impregnable defense that will keep all attacks out. And I don't think you have been saying that. We certainly need to try and have the most established firewalls, but the key is also to be prepared to recover when there is an attack, and that takes a tremendous amount of work as well.

Mr. CLAY. Can any other panelist give me a sense of the scope and nature of the types of cyber attacks that we are seeing from China, Russia, North Korea, and Iran?

Mr. Healey, any sense of—

Mr. HEALEY. Yes.

Mr. CLAY. —the scope of the attacks?

Mr. HEALEY. Yes, sir. Certainly, what we have seen—the Verizon data breach investigations report, which was already brought up, does a good job of seeing the kinds of attacks that have been hit-

ting the finance sector as a whole. The larger set of attacks hitting the finance sector has been point-of-sale and other kind of similar attacks are those that go like phishing emails after Web sites.

What is surprisingly small for the finance sector has been inside abuse, which has been only about 7 percent of the total, and also espionage, which again we tend to associate with China, has only been about 1 percent. So really, cyber espionage hasn't been the scourge for finance as it has for some of the other sectors.

Russia, Eastern European hackers, because they dominated a lot of that criminal market has been I think a lot more significant than North Korea or China. Again, we saw Iran very significantly 2, 3 years ago and we may see them again.

Mr. CLAY. Mr. Fitzgibbons?

Mr. FITZGIBBONS. One thing I would add is there is an important point here, and that is really regardless of the threat, and those threats that you have referenced are certainly recognized, the defenses against it often are very, very similar. And they come down to some very, very basic fundamentals.

Mr. Healey referenced phishing attacks and so forth. That still is probably the single-most prevalent form of attack against institutions. So regardless of where that attack is emanating from—the training, the education, and the discipline around infrastructure and security, et cetera is really the best way to ensure that regardless of the threats that we are protecting ourselves to the greatest extent.

Mr. CLAY. Thank you so much. Mr. Chairman, I yield back.

Chairman NEUGEBAUER. I thank the gentleman. We will now recess. We have four two-vote series. I encourage all Members to return as quickly as you can, and we will get started as soon as we get back.

With that, this hearing is recessed, subject to the call of the Chair.

[recess]

Chairman NEUGEBAUER. The committee will come back to order. And I now want to recognize the gentleman from New Mexico, the ranking member and past Chair of the subcommittee, Mr. Pearce, for 5 minutes.

Mr. PEARCE. Thank you, Mr. Chairman. I am trying to re-register. Maybe I will stay where I am at.

So, Mr. Fitzgibbons, Mr. Healey said that looking ahead, we need not be overly concerned with large-scale attacks that might seriously disrupt the economy. Is that something you would agree with?

Mr. FITZGIBBONS. I would agree to a point, okay. I think when you look at the nature of the attacks and what is possible and what is potential, we tend to look at things as what is going to be the extreme, what is the worst, worst possible scenario.

So while I might agree, kind of conceptually or theoretically, that that is maybe not likely, you have to prepare regardless. So when we are actually doing our analysis and also with our regulatory authorities, they are actually asking us, how would you recover from that extreme event they referred to as extreme yet plausible. So while I agree with the concept, we prepare for the catastrophic attack.

Mr. PEARCE. Mr. Bentsen, you also said that transparency and regulations—the regulations should move towards transparency, is that more or less it? Is that something you would also agree with?

Mr. BENTSEN. I think transparency and harmonization—I think some of the other panelists mentioned this beforehand. I have members who are bank-affiliated broker-dealers and futures commission merchants, so they are regulated by three prudential regulators as well as the SEC, the CFTC, FINRA, and the National Futures Association. All of these agencies appropriately are looking at guidance and regulation with respect to—an inspection with respect to cyber defenses in the firms. And we believe there should be harmonization across those agencies.

Mr. PEARCE. Now, as I listen, as you can tell, I don't have a Ph.D. in cyber warfare, but it seems like we are mostly on defense and cyber warfare. In other words, we are like goalies on a dart team trying to catch the dart before it sticks in the board behind us. Do we ever have any offense like when they get into our systems? Do we have malware that is waiting for them to greet them and go into their systems and start?

Mr. Garcia?

Mr. GARCIA. No, sir. That is illegal. Offense from the private sector side is not a legal thing to do. So that is the purview of the department.

Mr. PEARCE. Do we prosecute people? Do we—

Mr. GARCIA. Prosecute, yes. As they are—we work closely—

Mr. PEARCE. How many—

Mr. GARCIA. —with law enforcement.

Mr. PEARCE. In a given year, the prosecutions might be what percent of the people who are trying to get into our systems?

Mr. GARCIA. Good question. I don't have that figure.

Mr. PEARCE. Anybody? Mr. Healey?

Mr. HEALEY. On the earlier question and shooting back, this is something that the Department of Defense has taken very seriously. And now they have a national mission for us at U.S. Cyber Command that is there looking into what they say, red space, looking at the United States' main adversaries. And if there were a large-scale attack on the United States of the kind I talked about, U.S. Cyber Command would be there to try and disrupt the incoming attacks on the finance sector.

Mr. PEARCE. Okay. And you feel like that has validity because in your closing statement you said that really you weren't looking for the military ninjas or something like that, cyber ninjas. And so you would feel like that offensive capability has some validity?

Mr. HEALEY. Yes, I am very pleased. It is there. I think if we were able to get more response in place and think more broadly, we might be able to get to fix the sector before it reaches the point that the Department of Defense needs to shoot back and potentially escalate the crisis.

Mr. PEARCE. Okay. So if we look back to the question of prosecution, do any of you know what the penalties are? In other words, are they sufficient to keep people from trying? Does it sound like we are too active in prosecuting people who carry out cyber warfare. Is that correct?

Mr. GARCIA. I think there is a bit of feeling that law enforcement could always use more resources and higher penalties so that they can really go after the cyber criminals.

I would also suggest though that there are other innovative ways of using existing law. In the past, the financial sector has partnered with companies like Microsoft. And as Microsoft sees everything that is happening on its platforms, the Hotmail and Windows, et cetera, they can see where some of these networks of cyber criminals are operating and how they are attacking financial institutions and together—

Mr. PEARCE. Okay. I need to get on another question. We are running out of time. They all are staring at me. The concept of—James Rickards in his book talks about how in 2009 the Pentagon sponsored a fairly significant cyber warfare on our financial institutions using stocks, derivatives, currencies. Is that—Mr. Healey, was that a process that was beneficial and is it still ongoing? Do you know?

Mr. HEALEY. I'm sorry. The 2009—

Mr. PEARCE. Yes, it was just the Pentagon sponsored a really significant mock warfare in the cyber theater.

Mr. HEALEY. Yes. Those kinds of exercises, I think, have been very interesting in getting some lessons that have fit in. But again, I think we often go to those extreme cases, which I think are less likely—are going to be—

Mr. PEARCE. —a small amount.

Thanks. I yield back.

Chairman NEUGEBAUER. I thank the gentleman. And now the gentleman from Massachusetts, Mr. Lynch, is recognized for 5 minutes.

Mr. LYNCH. Thank you, Mr. Chairman. And I want to thank the witnesses for your help today.

I have my doubts about how well-prepared we are. Back in 2010 we had the flash crash, of course, and the market plummeted 600 points in a couple of minutes and then it came right back up. And we did a full study, the CFTC and the SEC, and they told us it was a firm here in the United States, and it was a result of certain trading patterns from that firm.

And then last month, so that was the story they had been giving the Financial Services Committee for the past 4 years. And then they did a further analysis in April of this year. They came out and said that was all wrong. It was actually a fellow named Sarao, a U.K. trader, who was spoofing and doing thousands and thousands of trades. So we had this whole narrative of 4 years about what they found was the problem with the system, and it was all hogwash. And finally 4 years later we find out—we think we find out what the real story is.

So I am just very skeptical that we have a good and strong assessment about the weaknesses in our financial services electronic trading and commerce in general.

Am I wrong in being suspect of the handle that at least the CFTC and the SEC have on all of this?

Mr. Healey?

Mr. HEALEY. To some degree, I certainly agree with you. The system has become so complex that it is difficult for anyone to try and

understand it. At least when we had—just trying to understand financial risk prior to 2008, we had risk modelers, we had VAR, we had all sorts of tools and people whose responsibility it was to track this complexity and figure out who was holding the risk at the end of the day.

I am worried that on cyber risk, not just in the finance sector, the system has gotten so complex that we can't model what we know who is ultimately holding the risk at the end of the day. And I think the sector has started to get their arms around this by looking at vendor management, active contact management to figure out not just how is the security at a single bank, but how is the security of their supply chain and those they depend on.

So we are starting to get our arms around it as a sector—

Mr. LYNCH. Yes.

Mr. HEALEY. —but I think it is very difficult.

Mr. LYNCH. Yes. I actually want to compliment the Chair of this subcommittee and the Chair of the full Financial Services Committee. We have been calling for these hearings just to look at cybersecurity for a little while, and they have been very responsive. This is the second hearing we have had in a couple of weeks.

Is there—I do want to talk about the financial services part of this, though. That is the one that we are principally involved in. And is there a moral hazard in the way we are handling this? Have we incentivized companies, especially JPMorgan Chase and others who have the reputational risk if their system is compromised?

Have we really—it seems like, with the Target hack and JPMorgan and others where you have had social security numbers compromised widely, there hasn't been a lot of downside for them other than the fact that some of their investors are probably worried about their personal information?

Mr. Bentsen?

Mr. BENTSEN. I would say two things about that, Mr. Lynch. Number one, every time those firms have a situation with information being stolen or we don't represent the consumer side of the business, but credit card numbers being stolen, it is those firms that underwrite the cost of doing that. So I think that if you look at the cost to the firms that they were having to absorb, and that is—and it is the right thing to do for the benefit of maintaining the confidence of their customers.

A second point I would make—and I take your point about the flash crash. And as you know, the regulators are in the process of putting in a consolidated audit trail, which the industry will pay for ultimately. It would be a mistake if the industry wasn't doing what it is doing right now and has been doing to map out what is going on to look and see where the vulnerabilities are, to look and see where the risks are with third party vendors across the spectrum.

And so, we may not be there yet, but I think you have to take stock of what is being done right now.

Mr. LYNCH. Okay. Thank you.

Mr. NICHOLS. I would add to—echo Mr. Bentsen's point about restoring trust with the consumer, it is a critically important thing and financial institution can operate without it, of course. But I would say to your point, it is extremely challenging.

The institutions have to be right all the time.

Mr. LYNCH. Yes.

Mr. NICHOLS. The bad actors can only be right once.

Mr. LYNCH. Yes.

Mr. NICHOLS. But I will say that all the institutions have made cyber defense a number one public policy priority.

Mr. LYNCH. Okay. My time has expired. I yield back.

Thank you, Mr. Chairman.

Chairman NEUGEBAUER. I thank the gentleman.

And the gentleman from Oklahoma, Mr. Lucas, is recognized for 5 minutes.

Mr. LUCAS. Thank you, Mr. Chairman.

Listening to you—to the panel, I suppose the one observation I would offer up is that in the nature of criminal activity, the desire of the criminal, of course, is to bleed the process, but not to kill the patient—to be able to return and bleed the patient again. Cyber activity that is nationalistic in nature, my phrase, clearly is out to inflict economic damage, to kill the patient.

So in the spirit of that, take me back to the fundamental rudimentary issues here. Describe for me how these kinds of attacks unfold in the fashion we are seeing now. And I don't care which member of the panel discusses it—how these cyber attacks unfold on financial institutions from the perspective of criminal activity or the perspective of a nationalistic effort.

Mr. HEALEY. If I can, I will take the national part, just to get us warmed up here.

So we have seen a number of these national state attacks that have looked at the finance sector. The most recent one where denial of service attacks by Iran, probably about 2012 that unfolded over the course of a year, almost 2 years of whether or not they were angry at sanctions and decided the finance sector was the right target to show their displeasure or out of—because they had been attacked by Stuxnet. So a group that was difficult to pin directly on Iran, but intelligence was able to help determine that it was.

Every day, every couple of days would decide on a new set of American banks that they would target. They would direct Botnet zombies under their control of compromised computers onto those targets every couple of days. They would change those targets to flood the Web site.

This wasn't a big deal if it was only interrupting getting to the main Web site of the bank. Again, it might hurt consumer confidence a little bit, but there is no real information that is important to the market.

If it was keeping them from getting access to look at their account, their online information, then it starts getting a little bit worse. Still not systemically important, because they can still get their money from the ATM; they just can't look at it online and do some of the bill pays or other things that they might want to do. That has been, I think, one of the best examples.

When the United States has wanted to do it against others, we have looked at, can we do covert actions, say against Slobodan Milosevic or Saddam Hussein. And we still—we love that idea, but it doesn't appear like we have done it just yet.

Mr. LUCAS. Gentlemen, on the criminal side?

Mr. GARCIA. I could—a common form of attack that can happen in any major organization is—as was alluded to before, a phishing attack. An employee receives an email that looks like it is from her boss or from a customer or from somebody they know and trust, and it looks authentic. They open the email and perhaps there is an attachment. Maybe they were even expecting that attachment.

And once it is opened, that actually turns out to be an attachment that is owned by the cyber criminal that then deposits into the computer system of the recipient some form of malware, a Trojan or some kind of a virus that then propagates throughout the corporate system. And then once they are in, they can browse around the corporate network and see where there is data of value, and you steal it, corrupt it, destroy it, and that is very common, and it is getting more and more sophisticated.

Mr. LUCAS. So the volume of attacks, I think was alluded to earlier, are increasing. At what rate would you describe from the criminal perspective this increase and is it from a dramatically different set of sources?

Mr. GARCIA. The increase—the potentially good news about the increase is that we have increasingly sophisticated tools to detect malicious activity. So having greater situational awareness about what is happening to us is a good thing, and then we can start—we can continue to tailor tools to combat that.

So, I think the vexing thing about technological innovation is not only does it give us great new tools for working and living, and playing, and entertaining, but it also gives enterprising criminals new sources of vulnerabilities to exploit.

Mr. FITZGIBBONS. Congressman, if I could just add one of the things that the increasing number of attacks certainly is important. But as we increase our defenses and can kind of recognize an attack and stop it, that is great. It is really the sophistication of the attacks and using the examples such as the phishing attack.

One of the things that we have seen whether it be nation-state or whether it be criminal is these attacks are very, very well structured. They obviously have information or they have information that suggests they understand your infrastructure. They understand your processes.

So your employees, your staff will be getting an email that you actually expected. You have heard that there was an upgrade to your email system and you are hearing from the systems administrator that, oh, in order to actually successfully move you across, we need to do this. And that is really the challenging part, because we can stop something that we know about and send it 100 times while stopping 100 times.

But when they find those backdoors and those side doors that take advantage of people's understanding of how their own company works, that is where it gets physically challenging.

Mr. LUCAS. Thank you.

Chairman NEUGEBAUER. The time of the gentleman has expired.

The gentleman from Washington is recognized for 5 minutes.

Mr. HECK. Thank you, Mr. Chairman. I want to add my voice to that of Mr. Lynch's expressing my appreciation for conducting this

hearing on what I consider to be a very important subject. I appreciate it very much, sir.

I don't know to whom I should address this question. I am going to try Mr. Garcia, just randomly here as a follow up to some of Mr. Lucas' line of inquiry. Do we have a rough sense about what the division is between nation-state attacks and domestic criminal attacks on cyber systems?

Mr. GARCIA. I don't have specific numbers, but I think cyber criminal attacks are much more numerous partly because there is a big business behind actually providing hacker tools to people who want to buy them.

Mr. HECK. So a majority of the attacks come from criminals domestically?

Mr. GARCIA. Yes.

Mr. HECK. So now I want to pursue—also as a follow up to Mr. Lucas kind of the accountability link here. I am not an IT professional, and I don't follow this as closely as those who are in the business do. But I have a simple if not simplistic view, namely cyber attacks cost money, destroy things of economic value. Just as certainly as if you were to know that I did—I was not within my home nor any of my family, but you burned it down. You would cost value, economic consequence.

And yet the truth is—I think I have read one or maybe two instances of somebody going to jail over this stuff. Now, look I realize we are in the midst of a legitimate debate about whether we are putting too many people in jail, certainly for non-violent crimes, but these have enormous economic costs. Do we have the legal framework to provide accountability for people who are destroying things of value, our time, our effort, our resources, to hold them to a standard of accountability that might disincentivize what is otherwise clearly an exploding field of the malicious activity?

Would anyone care to respond to that?

Mr. FITZGIBBONS. Congressman, that is a terrific question. And one of the challenges, one of the discussions we will often hear is these are crimes without consequence. It is a great business case, do a cyber attack and what is the chance of getting caught.

I think that is a bit unfair because when we speak with law enforcement, they are working very hard to try and get at these folks. I think—

Mr. HECK. Are the perpetrators being indicted and jailed?

Mr. FITZGIBBONS. There are indictments that are actually being passed against the people who are actually outside our borders. And when those opportunities present themselves, apprehension is actually taking place. I think one of the things that we enjoy is when we do have these opportunities to speak with law enforcement to hear more about what they are trying to do.

Having said that, we want to see more from the private sector. We do want to see more consequence. We do want to see more prosecution. We do want to see more people being held accountable, but we recognize they are somewhat complex given the happening outside our borders and it is not easy to do, but the dialogue between ourselves and law enforcement is very good in terms of, we have a common objective.

Mr. HECK. Do we have an adequate statutory framework?

Mr. HEALEY. I believe in the United States we do, sir. I think the statutory framework here goes back something like 30 years. It is very solid. The law enforcement agency has been catching up.

What worries me and probably the whole panel is there are sanctuaries. If someone is hitting you from China, you are probably never going to get them. If someone is hitting you from Russia, you are probably never going to get your hands on them, and so they are able to operate from these sanctuaries with—

Mr. HECK. What could we do?

Mr. HEALEY. Russian Mafia with ties to the Russian government—

Mr. HECK. No, no, no, what could we do to disincentivize this behavior?

Mr. HEALEY. I think put pressure on the governments where we can, try and include this into our overall conversation.

Mr. HECK. Diplomatic pressure.

Mr. HEALEY. And also just—

Mr. HECK. How is that working out for us?

Mr. HEALEY. We are never going to get cuffs on them, sir, so I think the more that we can do to disrupt their operations, things like botnet takedowns, try and increase the cost on them so that way—if we can't put the cuffs on them by putting them in jail, we can increase the cost so it becomes more and more and more difficult.

Mr. HECK. I have one last question quickly. I see my time is dwindling. I am interested in whether or not our emerging new payment methods, whether it is Apple Pay or Google Wallet, how has this increased our exposure? What is the trend line? Are we seeing an expansion of attacks associated with these new payment methods diminished within that segment of payment, holding—comparable to other means? Are we more exposed, less exposed? What is the trend line?

Mr. FITZGIBBONS. Maybe I will take a shot at that, Congressman. I think when we see innovation in the payment space such as Apple Pay and those other things, from a payment system perspective, we welcome innovation. A lot of this innovation is really being driven by just those threats themselves, taking account numbers and personal identifiable information out of the mix.

But having said that, the adversaries are very, very quick to adopt to different things so they will look for weaknesses in that and we need to remain ever vigilant that we actually are going after them.

One thing I would mention there is that in the payment systems there is a huge amount of regulation and understandably so. When we look at some of these other service providers and we are talking about something as important as cybersecurity, are they subject to the same regulations? So that is something that needs to keep pace for the reasons that you were just referencing.

Mr. PEARCE [presiding]. The gentleman's time has expired. The Chair now recognizes Mr. Pittenger from North Carolina.

Mr. PITTENGER. Thank you, Mr. Chairman. And I thank each of you for being here and for your valuable time.

As we consider the stability and the viability of our financial markets and financial institutions, what concern do you have for

our electric grid, the important factor that plays? Who would like to respond to that?

Mr. BENTSEN. I will start, Mr. Pittenger. I think every sector, every critical sector, critical infrastructure is working on this. I obviously can't speak for the others. But we are concerned from our standpoint of making sure that those sectors are equally protected or taking the necessary steps to provide defense.

As one of my members had said before, if the Fed wire is down, we can probably work around it. But if we don't have power, we really can't do anything at all. And I think the same would be true with other critical infrastructure like the telecom sector.

We can talk a lot about the financial services sector and the work that is being done, and I think there is a lot of work being done, but we have to take into consideration that we are connected to these other critical sectors.

Mr. PITTENGER. Sure. Would anyone else like to comment?

Mr. GARCIA. Yes, sir. The Financial Services Sector Coordinating Council has embarked on some cross-sector initiatives to engage particularly with the electric sector and the communication sector.

First, to just understand what our interdependencies are, what our mutual vulnerabilities are, and then think about ways that we can collaborate in areas such as joint exercises in the event that the power goes out; how will that affect our respective sectors. So it is a positive cross-sectoral engagement going on.

Mr. FITZGIBBONS. One thing I would add to Mr. Garcia's statement is it was very interesting that when we were reaching out recognizing this cross-sector requirement, we can't just be an island into ourselves. We often enjoy this reputation of being kind of out in front and so forth. But again, to your point, the other sectors, we are all dependent upon each other. So when we were actually reaching out to the electric sector, they were literally picking up the phone to call us as well.

And I think that really does speak to how very broadly these threats are actually being taken by all the critical infrastructure. So I think there is a good news for you in that.

Mr. PITTENGER. About a month or so ago I was in Israel and met with some of the individuals who have been playing an active role in securing their grid through a cyber war. And then subsequent meetings in Vienna and back here a week or so ago, they will be here. And I would just like to personally invite you to come. This will be a Members' meeting, but it will be one that you would be most welcome to come to, on June 2nd at 4 o'clock.

And the head of the National Cyber Bureau who works directly under the Prime Minister will be here to address this issue and show us what they have done to seek to secure their grid from cyber attack.

On another matter, Mr. Healey, given that we have limited extradition treaties with certain countries, particularly in Eastern Europe, what other ways can we seek to justice against these individuals if we don't have extradition treaties and the limitations there?

Mr. HEALEY. Justice is going to be very difficult and, in fact, might be unattainable. So we have to look for other positive public policy outcomes that we can achieve.

The sector, I think, has done a good job in working with the telecommunications sector, ISPs and others, vendors like Microsoft in asking, how can we disrupt their attacks to begin with? That doesn't give us the satisfaction of seeing the punishment that they deserve, but it can stop the attacks from having the effect that they want on the sector.

I am very hopeful that now that the White House has come out with their plan for information-sharing and analysis organizations, we can use these kinds of groups to be more purpose focused.

I have not spoken much about information-sharing. I don't care much about information. I want to see results. And so if we build our groups around stopping DDoS attacks, stopping account takeovers and the rest, and build our information-sharing to that, I think we can thwart them much better than we have been.

Mr. PITTENGER. Certainly. I yield back. Thank you.

Chairman NEUGEBAUER. I thank the gentleman. Now the gentlewoman from New York, Ms. Velazquez, is recognized for 5 minutes.

Ms. VELAZQUEZ. Thank you, Mr. Chairman. I, too, want to thank the chairman and the ranking member for holding this important hearing.

Mr. Garcia, if I may, what is being done by the public and private sectors to advertise the importance of cybersecurity to the small business community? Also, what cost-effective steps can they take to protect themselves and their customers?

Mr. GARCIA. That is a very good question. Thank you for that. There actually is quite a network of private sector organizations that are thinking regularly about how to get those tools and awareness into the hands of small business owners and consumers.

There is an organization called the National Cybersecurity Alliance; one of our member institutions is on the board. They host, along with the Department of Homeland Security, every October, National Cybersecurity Awareness Month and it is a major national campaign. All 50 governors declare—

Ms. VELAZQUEZ. Are you aware of any coordination with the Small Business Administration?

Mr. GARCIA. Yes, and the Small Business Administration is a part of that. Many major—many of the Federal agencies are a part of it and our own Treasury Department and some of the Federal regulators for the financial institutions reach out to the small banking community institutions to raise awareness there.

And the National Institute of Standards and Technology has developed a framework called the NIST Cybersecurity Framework, which we are helping to push out to the small institutions. And that is one of the cost-effective tools. It is simple. It is scalable, and it gives them a sense from the IT administrator up to the CEO what their responsibilities are for managing cyber risk.

Ms. VELAZQUEZ. Thank you.

Mr. Nichols, the nature of the U.S. card market presents unique challenges as we move forward with EMB implementation. As you know, many of the 28 million small businesses in the United States now accept card transactions, and switching over to card reader technology will be costly. Is there anything being done to help mitigate the costs and also to inform the small business community of the risk of not upgrading?

Mr. NICHOLS. Upgrading to—did you say chip and PIN? Okay.

Ms. VELAZQUEZ. The new technology.

Mr. NICHOLS. Yes, sure. I guess, an observation on that, it is obviously—I will talk about the underlying technologies for a second. It is a good technology. I would say that there is probably no single technology that will prevent all breaches. We have talked at length today about the creative and inventive ways that the bad actors participate in this market.

We are also mindful that the government doesn't inadvertently stifle future innovation by speaking to—overly praising one particular technology, in part, Congresswoman, because innovation is moving so quickly at such a rapid pace not just in payments but in other aspects of the financial sector and the general technology community.

Who knows what tools we are going to need 5 years from now, 10 years from now, 15 years from now or 20 years from now. The space is so rapidly changing, looking so dramatically different. So we need to keep—we obviously—we need to keep pace with whatever the latest technologies are.

It also underscores a point I made very briefly earlier about the priority level that this is within the financial institutions in America. The leaders of these financial institutions are saying things like, no expense will be spared as it pertains to our cyber protections.

Another leader said that in an area where they are doing lots of cost-cutting, this division of the company never needs to ask permission to spend more money. It is a huge priority getting this right. And it is something that these institutions think about each and every day.

Ms. VELAZQUEZ. Thank you.

Mr. Bentsen, we all know that Federal spending to combat cybersecurity continues to grow at an extremely rapid rate. How do we tap the unique talents of small technology firms in an effort to strengthen our national cybersecurity defenses, especially in the financial sector?

Mr. BENTSEN. That is a good question, Ms. Velazquez. I think that this is a problem that is not unique to the largest firms both in terms of the largest banks or the largest technology providers, and there is a tremendous amount of work that is being done to look at it because this is such a priority.

And so I think you are right that we—the industries—are going to have to look at who is going to be coming up with better mouse traps as we go along in this process. And it is important that we don't, to follow on to Mr. Nichols' comments, in a broader context, not in the chip and PIN, that is not really in our space that we don't stifle the ability of tech companies, startups and others to work on this. There are quite a few in this space today, and we hope that there are more down the road.

Chairman NEUGEBAUER. I thank the gentlewoman. The gentlewoman's time has expired.

The gentleman from Colorado, Mr. Tipton, is recognized for 5 minutes.

Mr. TIPTON. Thank you, Mr. Chairman. I would like to thank the panel for taking the time to be here. Ms. Velazquez and I have a common interest in small businesses.

And, Mr. Garcia, you just mentioned that there was a big effort to be able to get information out to those small businesses. What is the participation level? Do you have any idea?

Mr. GARCIA. The FSSCC has a Small Institutions Outreach Working Group that is—that involves the Independent Community Bankers of America, and several other trade associations are involved, and several other companies. And we are thinking about, how do we get their attention when you have small bank CEOs who are really focused on running their business. And now we are asking them to think harder about cybersecurity and how to manage their third party service providers.

We are working closely with our government counterparts in Treasury and the FFIEC to consider the best strategy for pushing out the best, simplest, scalable—

Mr. TIPTON. I am just kind of curious. Do you have any idea—you know, if we have 100 percent independent bankers? X percent participate in some of these rollouts. Is there any way to be able to identify that?

Mr. GARCIA. I wouldn't have that information. Perhaps maybe some of my colleagues—

Mr. BENTSEN. Yes, sir. I would just add to that on the broker-dealers and asset management side, to your point, SIFMA and our membership made a decision to underwrite membership for our smallest firms, 6 percent of our member firms have less than $200 million a year of revenues, but for the smallest firms, membership in FS-ISAC because we want 100 percent participation.

And to be fair, it has been painstaking to get these firms in because in some cases you have—the CEO is also the chief technology officer in a very small firm. So this has been sort of almost a one-on-one communication.

Likewise, we have been working with those firms on what their insurance policies are, how they can—whether they can come together to buy insurance policies together, what they have in their insurance policy. And we have encouraged the regulators, FINRA, for instance, who is the self-regulatory organization for broker-dealers, to work with the smaller members in this process.

Mr. TIPTON. Great. Mr. Nichols, do you have any comments on this?

Mr. NICHOLS. No.

Mr. TIPTON. No, okay. Great. Just as a little bit of follow-up on this, with smaller institutions, can they be a gateway to the bigger institutions when we are looking at the cybersecurity? Does that stress the importance of getting this information?

Mr. BENTSEN. Absolutely. Everybody is a gateway. Everybody is linked together in the trading world or on the bank side. And that is why we did our diagnostic and worked to develop standards that would apply across the industry because they clear with others, they trade with others, and that is why we want to make sure everybody is in the information grid, that everybody's insurance is up-to-date. And so it is something that, and I know that the bank-

ers are doing the same thing, we have to get universal adoption within the industry.

Mr. NICHOLS. Congressman, I would add just very briefly to that. In my written testimony, I talked about this issue of the automated programs and all the investments that are being made there. Kind of two points apply here.

One, what does that actually mean in layman's terms? I am not a cyber expert like these two guys are. But in layman's terms, is it that we are trying to get the financial system to operate like your body's immune system, so that it fights off the illness before it gets there? So one, these programs allow you to quickly differentiate a small attack or a low priority attack versus the really serious stuff, the really wicked and malicious stuff. So that is kind of half of what it does.

And the second half of what this automation, these programs and systems does is quickly and swiftly disseminate the nature of the threat across the system to institutions of all sizes. And that is where a lot of the large financial institutions are making investments that help not only themselves and their clients and customers, but people all across the spectrum.

Mr. TIPTON. Right. Thanks.

Mr. Garcia, something I just wrote down as you were speaking, giving your testimony was the need for more uniformity, and examinations regarding—is there duplication? Is there overlap? Are there additional costs that are being driven that could be better spent on cybersecurity?

Mr. GARCIA. Yes, I think that is our experience and it is anecdotal, but one company could have several different regulators, depending on their various businesses. And the examiners who come in have different sets of questions. And they are all getting to the same issue—security and resiliency—but we have to answer the questions in different ways.

Our point was if we could harmonize, as Mr. Bentsen said, across all other regulatory agencies, we could have the same sets of questions. We could focus on actual security and resiliency and not answering questionnaires or answering fewer questionnaires.

Mr. TIPTON. And just one final question here, Mr. Fitzgibbons, you mentioned about the recovery process by small and medium-sized firms after an attack. How does that compare to a big firm? I think I know the answer, but what are some special challenges our smaller firms are facing on a recovery after an attack?

Mr. FITZGIBBONS. Congressman, thanks. It is an interesting question. Many of the regulations that the larger firms have to deal with actually require a significantly accelerated recovery time. So it is almost as if the bigger the bank, the faster you can actually recover. A lot of that is driven by regulatory requirements. A lot of that is driven by the sophistication and the investment they make in a lot of technology. So significantly, systematically important, financial institutions actually recover very, very quickly from outages.

The small and the medium-sized institutions may not have that regulatory mandated requirement. Having said that, the way that technology is shared, the way the technology evolves and so forth,

recovery out of various critical systems and so forth, be it the payment system or DDA system—

Mr. TIPTON. Yes. Thank you, sir. I yield back.

Chairman NEUGEBAUER. I thank the gentleman. And now the gentleman from Texas—

Mr. WILLIAMS. Thank you, Mr. Chairman. I thank you all—

Chairman NEUGEBAUER. —is recognized for 5 minutes.

Mr. WILLIAMS. —for being here today. I think for me, as someone who comes from a small business background, this issue is clear. I think I can give you a little unique perspective on this topic.

As retailers, your ability to sell a product is everything, as you know. Once you lose that ability, you damage your reputation, and you limit your ability to be truly successful.

In my instance, I just happen to be a small business owner; I am a car dealer. My customers trust that whatever information they share with me is protected. The Federal Government doesn't need to tell me that. But whether it is my industry or something else, gaining and keeping customers' trust is vital. Without that trust, you might as well not be in business.

Now because the debate is really about making sure the customer is protected first and foremost and giving them the best service possible, I think is what we have talked about today.

So let me bring this up. In 2014, the auto industry and the National Highway Traffic Safety Administration came together to create a sharing advisory center, known as Auto ISAC, to share cyber threats among 34 auto manufacturers. The idea is for automakers to share information about attempted security breaches so they can be neutralized quickly. Also, the Society of Automotive Engineers established the Electrical Systems Security Committee, which is created to review challenges, and capture solutions standards to prevent cyber attacks in current future vehicles.

As a car dealer myself, the coordination of my industry and the Federal Government is encouraging because again reputation is everything. I believe they have seen what has happened in the retail and financial sectors and try to be proactive. With mobile devices like Wi-Fi and other technologies almost commonplace in vehicles, the bar needs to be high.

So can any of you on the panel comment on what the auto industry has done and how this might be a helpful model for other financial industries when coordinating information-sharing with the Federal Government? Any of you?

Mr. HEALEY. Sir, a lot of the ISAC dates back to 1998 when President Clinton asked because, of course, he couldn't tell the private sector to come together and put these ISACs in place for their sectors.

The finance sector started the year after—1999 was the Financial Services, ISAC. I had the honor to be vice chairman of that group several years after that. So a lot of the—the finance sector is one of the few that of those original set that is kind of going strong. Telecommunications has been good. Information technology has been good.

Many other sectors, they have kind of been born and died in the time before auto came together. So I think auto is in a great posi-

tion of having been able to look at what has worked best in these ISACs and what hasn't.

For example, in the early days of the financial services ISAC, we wanted to jump right into automated sharing of the kind that we heard about today with Soltra Edge. But we weren't ready, we didn't have the trust between us yet. We had to sit down together, get to know one another, have a few drinks together, and then we built up that trust between ourselves and with government.

Also, one of the big lessons is a higher level of governance for the sector. The ISAC was operational only. Then, when we had to deal with the government on larger issues, we were too operationally focused to have that. So, we came up with a group that Greg now represents, the FSSCC, to be there at that higher level and the regulators set up the FIEBC, their structure, so that we had this government regulators and finance sector policy level, at the managing director level to cooperate.

So I think the Auto-ISAC is on great ground and I look forward to seeing what lessons that finance can draw from it.

Mr. WILLIAMS. Thank you very much.

Mr. Bentsen, you said in your testimony that Congress needs to remain proactive and vigilant on the topic of cybersecurity and that passing legislation is needed for the financial industry. Does the Federal Government need to mandate policies on sharing cyber threats again, as we can see the auto leaders and the Federal Government are already working together without Congress telling them to do so?

Mr. BENTSEN. I think in the case of information-sharing and giving, and liability protection, FOIA, which the House has done, is very important. The industry is certainly working within the law as it is today, but it would be that much better if the other body would move forward in passing the CISA bill and getting it to the President's desk.

I think beyond that what we called for in our recommendations is for the Federal Government—the regulatory agencies to look at what the industry has done and create guidance out of that, and do it across the agencies in a harmonized way. So to the earlier points that we don't have—our members don't have to have different guidance, different examination structures from regulators who are all seeking the same outcome.

And if there—to me, in dealing a lot of regulatory policy, if there was ever an example where regulators could come together on a uniform approach, this is it.

Mr. WILLIAMS. Mr. Chairman, I yield back.

Chairman NEUGEBAUER. I thank the gentleman. Now the gentleman from South Carolina, Mr. Mulvaney, is recognized for 5 minutes.

Mr. MULVANEY. Thank you, Mr. Chairman, and thank you, gentlemen, for doing this.

I am going to ask some simple questions, and I hope I know the answers in advance. But I just want to clarify this because, Mr. Healey, you got my attention during your opening statement, about one of your concerns—probably a valid concern—about the risks that the financial system faces in the event of some rogue international actor.

I think you specifically mentioned Iran or Russia being backed up against the wall, feeling they have no vested interest in the financial system, with very little to lose, especially since they could pull off some type of plausibly deniable type of effort.

So I guess, for the sake of starting the discussion, let me ask you the question then that should be first and foremost in everybody's mind, which is how safe is our money? If I have money in a particular financial institution—pick one of the major institutions—how safe is it in your opinion, sir?

Mr. HEALEY. I believe it is safe. The—

Mr. MULVANEY. Tell me why.

Mr. HEALEY. —I believe the American financial system is sound. I think it would be very difficult, as we also said in those opening comments, for any adversary to systemically disrupt the American financial system over a long period of time. It is just very difficult, I believe, in all of the strengths that we have talked about here.

However, particular institutions, well, one we might see shorter-term disruptions, maybe not being able to close at the end of the day like we would normally expect to.

Mr. MULVANEY. Mr. Healey, let me cut you off.

Mr. HEALEY. Sure.

Mr. MULVANEY. If you could take that to a retail level for me, because you understand what it means for banks not being able to clear at the end of the day. Sometimes I think I understand, sometimes I don't. What does that mean to an ordinary family?

Mr. HEALEY. Right. If the—especially if this kind of attack were to happen, for example, on the 15th of the month or the last day of the month at a particular institution, then I believe that—no financial institution, I believe, can stand up to the kind of attack that we might be able to see from one of these organizations.

That doesn't lead to anything systemic, but I think it is going to give a single bank a really bad day.

Mr. MULVANEY. Would anybody else care to weigh in on that?

Mr. FITZGIBBONS. I think when you talk about attacks on the financial system or financial institutions and then the impact on the family, there is impact. So it could very well be. It is—they are trying to make a payment, a bill pay or whatever it may actually be, and that actually gets disrupted. So they can actually feel that particular impact.

Coming back to the point about safe, having said that and recognizing there is the potential for attacks and potentially successful attacks, that doesn't mean that the system is unsafe. I think we need to keep it safe. I believe it is safe. I believe we need to make it safer. I believe that when we see a threat or there is a threat or an attack against a particular thing, what is important is how quickly we react to that, how quickly we isolate it and move forward.

Mr. MULVANEY. Thank you for that. That is a wonderful summary. Thank you both, gentlemen, for clarifying that because what I think we are saying is that while individual institutions may be subject to attack, that the system will remain strong, and that any impact on ordinary Americans would be temporary at worse. So it would be something that could be fixed in short order. I think it is important that we come out of this, Mr. Chairman, recognizing

the fact that the institutions are sound and it is still safe to put your money in the bank.

Now, let me ask a follow-up question. How safe is my personal information? I will come back to you, Mr. Healey, because I think you said you didn't care that much about it, but I may have—

Mr. HEALEY. No.

Mr. MULVANEY. I may have heard that out of context. So how safe is my personal information, especially in light of this world we are creating now? And I think we were inevitably there where you all have—different institutions have to share information. So how safe is my personal information?

Mr. HEALEY. I do not believe it is safe. We have seen the hackers be able to hit for decades to be mostly unstopped. Year after year, they have continued to make gains over us, the defenders.

Of the places where my personal information lives, I feel safest of where it lives in the finance sector. I am really happy that my bank has my social. I feel a little bit worse that the Social Security Administration has my social. I am pleased that student loans are with my bank. I am a little bit more nervous with the Department of Education.

That said, it is a deep concern. No one's information is safe.

Mr. MULVANEY. Anybody else? Mr. Bentsen? Mr. Nichols?

Mr. NICHOLS. I would echo Mr. Healey's observation. We are all at risk, even though the financial sector is widely acknowledged to have the best protections right now. But I echo your sentiment about the concern.

Mr. BENTSEN. Look, the industry has the greatest interest in protecting the information of its clients because if they don't their clients are going to go somewhere else. But it is extremely difficult.

I do want to say one—

Mr. MULVANEY. It would be hard to go to a different Social Security Administration.

Mr. BENTSEN. Well, perhaps. But I do want to add one other thing. I think the system is safe today. I think there is risk to markets and that could have impact in pricing. It could impact the individual investor. But I think we have to recognize that the people who are seeking to do this, whether they are individual criminals, or nation-states, or terrorists, or whomever they may be, they are getting better every day as well.

So it is the same person that somebody was trying—somebody is trying to pick a safe, they may not know how to do it now, but they are going to keep trying to get better and better, and so we have to keep preparing for the worst-case scenario.

Mr. MULVANEY. Gentlemen, thank you very much.

Chairman NEUGEBAUER. I thank the gentleman. Now the gentleman from Missouri, the chairman of our Housing and Insurance Subcommittee, Mr. Luetkemeyer, is recognized for 5 minutes.

Mr. LUETKEMEYER. Thank you, Mr. Chairman. It is kind of interesting that we have a TV show now, CSI Cyber. It is interesting that we have come that far.

I want to follow up a little bit on Mr. Mulvaney's remarks with regard to the security of information. But I want to approach it a little bit differently, from a standpoint of sharing the information between the various entities. How much individual information is

being shared between the different groups that are involved here whether it be law enforcement, whether it be the EFT transaction folks, the securities, banks, whatever? How much individual information is being shared there? None, a lot, everything?

Mr. FITZGIBBONS. So when—to talk information-sharing because often it is referenced as a way to share threat information, threat indicators and so forth to allow us to protect ourselves.

In that forum, and I can tell you from our strengths, when we are sharing threat indicator, we do not share personally identifiable information. That is not really what we are talking about. We are talking about information-sharing.

Mr. LUETKEMEYER. That is the point I want to get to here is that when we—you talked about information-sharing, the people watching this hearing today, the radar goes up like, oh, my gosh, the NSA is watching and now we have all these cyber guys out here watching. So I think it is important that you clarify that from a standpoint this is not individual information that you are sharing. This is more transactional activity that is being monitored by some outside group, and you are sharing that kind of information. Is that—

Mr. FITZGIBBONS. That is a terrific point, Congressman. Actually, I appreciate the opportunity to provide that clarity. Oftentimes, when you are dealing with these issues, you are speaking in terms that are kind of understood. But it is important to understand that when we talk about information-sharing as it relates to the threats, it is not PII, it is about IP addresses or different bits of code that you should be on the lookout for in your particular systems.

When there is an attack, what actually happens is PII will be very, very deliberately stripped out so that there is no sharing of that information—that specific information. So we are talking about threat indicators, not personal information.

Mr. LUETKEMEYER. Okay. Along that line, how much sharing goes on between industries? In other words, between the financials—the banks, the credit unions, the insurance companies, financial or securities folks. Between the industries, is there this information going on or only just between bank to bank or credit union to credit union, or insurance companies to insurance company? Can anybody elaborate on that?

Mr. GARCIA. Certainly, within the Financial Services ISAC, there are I think north of 5,000 member organizations now spanning the financial services subsectors. At the same time, the vice president of the FS-ISAC is Chair of the National Council of ISACs, so you have the electric ISAC and the telecom ISAC, and the financial ISAC.

Mr. LUETKEMEYER. Okay.

Mr. GARCIA. And they are all working together sharing information at a higher level, not at the level of detail and specificity that the FS-ISAC is, but that sharing is happening.

Mr. HEALEY. And the ISAC has taken on international members, so we are starting to work outside with our key financial partners.

Mr. LUETKEMEYER. Okay, very good. Thank you.

Along those lines, one of the reasons that we are having a hearing today is not only to determine the kinds of threats that are out there and what else going on, but also what tools do you need in

your toolbox to be able to fight this? Are there legal impediments—in other words, does Congress get some ability here to help you? Are there things that we need—that are in place right now that are hurting you? Are there things that we need to put on you to stop some of the stuff you are doing that may be beyond your scope or beyond what we really need to be involved in. It is kind of a long question.

But I think if you can give me an idea if you think there are some things that we can do to tweak the law or I am sure we haven't found a whole lot to probably go after anybody on, but along those lines.

Mr. BENTSEN. Congressman, again I would go back to the need for information-sharing given the liability employer protection would be important. Again the industry is concerned about PII; it is a customer confidence issue. But to do everything we need to do to protect the customer, we don't want to have the situation being second-guessd after the fact when you are trying to deal with an ongoing cyber attack.

I think beyond that, to the extent that the Congress can encourage the regulators to work collaboratively, and I think we are doing better at that, so we have harmonization, that will help the industry, as the industry itself moves to implement the standards and recovery protocols, and information-sharing as well as things like third party vendor verification or audit practices. And so I think that encouragement can help quite a bit, and then let the industry collaborate with the public sector, so we are talking to one another in dealing with how we respond to attacks, how we deal with recovery, how we deal with information-sharing.

Mr. LUETKEMEYER. Perfect. I see my time is about up. I will yield back, Mr. Chairman. Thank you very much.

Chairman NEUGEBAUER. I thank the gentleman. Now the gentleman from California, Mr. Royce, the chairman of the House Foreign Relations Committee, is recognized for 5 minutes.

Mr. ROYCE. Thank you, Chairman Neugebauer. I appreciate that.

Mr. Bentsen, it is good to see you, and the rest of the panel members there—Mr. Garcia.

I guess, as we get down to the nitty-gritty of how we get to where we need to go, you mentioned earlier the concept of having these different sectors work together. You all work with a number of Federal agencies or—including with the financial regulators, you work and have some knowledge of their expertise, since I think we even have a representative on the NCCIC (N-kick) watch floor.

So the question would be, for better coordination or harmonization, to get there somebody, in my opinion, has to be in charge. Somebody has to take the lead on it, and I don't think that has been asked yet. Maybe, Mr. Bentsen, you could start. Who should be in charge—Treasury, OCC, Homeland, DOD? How do you set this up? Because at the end of the day, unless somebody is in charge, bringing everybody together, it is awfully hard to make it work.

Mr. BENTSEN. That is an excellent point. My own view is—in our experience throughout this process is that—Treasury has a huge role to play in the financial sector. Obviously, DHS has a role to play, but does the national security apparatus, particularly as we

are talking about nation-state attacks or terrorists. So I think where the coordination needs to occur, and I would argue that it is occurring now is at—in the Executive Branch and in the Executive Office of the President because that is where the ultimate national security apparatus is. So you have to bring together the different groups.

It can't just be Treasury. It can't just be DHS. It has to be—somebody has to be coordinating at the top, and so that is where we are seeing in some of the exercises we are doing in working across the different agencies, not just the financial agencies.

Mr. ROYCE. The second question I would ask—I understand your concept there and where the decision-making—where the focus should be in the Executive Branch, but I still think you probably have to give most of the key decision-making to the entity that has access to the most information and understands it the best.

But in your testimony you also talked about the need to increase the pool of educated cybersecurity personnel. There are a lot of universities now involved in this sphere, including Cal Poly Pomona, which is in my district. But I am wondering what the industry is doing to address this particular workforce shortage in this area of expertise. Are you working with higher education institutions in order to churn out people?

I can tell you, on the other side, Moscow clearly is working hard and educating teams on the other side of this equation. Now they have that special bureau from North Korea that is out there educating right now in terms of how to hack into the South Korean banking system. So if we are going to do some good defense work, it is good to work through the university system as well in order to offset what is probably coming.

Mr. GARCIA. Yes, sir, Congressman, that is a great question. Within the FSSCC we have two task groups that are focused on that question. One is a workforce task group—how do we build capacity for cyber talent that we can use in the financial services sector and how do we describe the range of job responsibilities that we need—number one.

And number two, we have a research and development committee. And within R&D, you think about trying to drive funding—Federal funding—a lot of it through the university—research colleges and universities to work on some of those grand challenges related to cybersecurity. And in the process, you are building a pipeline of graduates and post-graduate professionals who will be entering the workforce, providing their level of expertise.

Mr. ROYCE. I am going to go back to Mr. Garcia and Mr. Healey's points. The concept of being allowed to hack back under strict controls, maybe being deputized by an accredited law enforcement agency, if that can be put together, is it a general consensus that it might be workable in terms of counter-battery work against those who are attacking these systems, any exception to that, or do you think it just might work?

Mr. GARCIA. An example that—perhaps stated in a different way was the financial sector's partnership with Microsoft where Microsoft was watching as was the financial sector all of the attacks on the Microsoft platform—

Mr. ROYCE. Right.

Mr. GARCIA. —like Hotmail and Windows.

Mr. ROYCE. You are not legally allowed—

Mr. GARCIA. They went to—

Mr. ROYCE. —to go on offense and you are saying they would be allowed to go on offense.

Mr. GARCIA. They cut off the command and control. They went to the U.S. marshal and got a court order to go to the command and control center where the servers were hosting these botnets and they severed that link.

Mr. ROYCE. Yes, yes. Okay.

Mr. Chairman, thank you.

Chairman NEUGEBAUER. I thank the gentleman. I want to thank our witnesses for your testimony. This has been a very healthy discussion. I hope the takeaway for the Members and even for some people who may be watching this hearing is that there is a lot of good cooperation going on within the industry because everybody has a vested interest here.

I think this is an ongoing dialogue. While we have only had two hearings here, I think this is an interest to our country from a national security standpoint, but also as far as protecting the financial network, which is so important to our economy.

Without objection, I would like to submit the following statements for the record: the Independent Community Bankers of America; the National Association of Federal Credit Unions; the National Association of Insurance Commissioners; and the opening statement from Mr. Hinojosa of Texas.

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.

And with that, this hearing is adjourned.

[Whereupon, at 3:12 p.m., the hearing was adjourned.]

A P P E N D I X

May 19, 2015

OPENING REMARKS
HONORABLE RUBEN E. HINOJOSA

FINANCIAL SERVICES SUBCOMMITTEE ON FINANCIAL INSTITUTIONS AND CONSUMER CREDIT

"PROTECTING CRITICAL INFRASTRUCTURE: HOW THE FINANCIAL SECTOR ADDRESSES CYBER THREATS"

MAY 19, 2015

RAYBURN 2175
1 PM

THANK YOU, CHAIRMAN NEUGEBAUER AND RANKING MEMBER CLAY FOR HOLDING THIS HEARING. I WOULD ALSO LIKE TO THANK THE DISTINGUISHED PANEL MEMBERS FOR SHARING THEIR INSIGHTS.

AS MR. BENTSEN STATED IN HIS TESTIMONY, "A LARGE-SCALE CYBER-ATTACK IS LIKELY THE MOST SIGNIFICANT AND SYSTEMIC THREAT FACING OUR ECONOMY TODAY."

OUR FINANCIAL INDUSTRY IS THE NERVE CENTER AND THE LIFEBLOOD OF OURS AND THE GLOBAL ECONOMY. OUR FINANCIAL INSTITUTIONS AND CAPITAL MARKETS ARE INTERCONNECTED LIKE NEVER BEFORE. A LARGE-SCALE CYBER-ATTACK ON THE FINANCIAL INDUSTRY OR ANOTHER AREA OF CRITICAL INFRASTRUCTURE CAN WREAK HAVOC ON OUR MARKETS, ECONOMY AND DAILY LIVES.

CONSEQUENTLY, TODAY WE GATHER INFORMATION IN ORDER TO CONSIDER OPTIONS AND ENSURE THAT OUR GOVERNMENT AND FINANCIAL INDUSTRIES ARE DOING ALL THAT IS POSSIBLE AND NECESSARY IN ORDER TO PREVENT SUCH AN ATTACK, AND IN THE CASE SUCH AN ATTACK OCCURS, TO MITIGATE ITS EFFECTS AND TO RECOVER FROM IT.

Written Statement of Kenneth E. Bentsen, Jr., President and CEO, SIFMA

before the Committee on Financial Services

Subcommittee on Financial Institutions and Consumer Credit

U.S. House of Representatives

May 19, 2015

Chairman Neugebauer, Ranking Member Clay, and members of the Subcommittee, thank you for the opportunity to testify today on such a critically important topic. A large-scale cyber attack is likely the most significant and systemic threat facing our economy today so it is appropriate that so much time and energy is being focused on developing public-private partnerships and identifying solutions to mitigate that risk. For SIFMA[1] and its member firms, our mission is to improve the collective ability of our sector to defend against a diverse set of cyber threats and be proactive in protecting our firms' clients and trading partners in addition to their data and networks from theft, disruption or destruction. Our member firms have invested huge sums of capital into their cyber deterrence and protection programs over the years and have enhanced their efforts to match the growing threat. From criminals seeking financial gain, to nation states committing corporate espionage, to cyber terrorists seeking to dislocate markets and destroy confidence, cyber threat actors are becoming more sophisticated, making cybersecurity an area of risk that must be actively managed by firms similar to all other areas of risk. The destruction of financial data including books and records or the disruption of our capital markets caused by a successful cyber attack would have a ripple effect across the economy and across the globe. As such, the financial services industry welcomes the importance placed on this issue by the Administration and the Congress, as demonstrated by today's hearing and previous hearings in the Financial Services

[1] SIFMA is the voice of the U.S. securities industry, representing the broker-dealers, banks and asset managers whose 889,000 employees provide access to the capital markets, raising over $2.4 trillion for businesses and municipalities in the U.S., serving clients with over $16 trillion in assets and managing more than $62 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.

Committee. As we focus on addressing the causes of the last financial crisis, it is equally if not more important that we focus on the future risks, and cyber is perhaps the greatest.

In order to insure adequate defenses and recovery protocols, it is critical that we establish a robust partnership between the industry and government as it is the most effective way to mitigate cyber threats: the industry will not be fully effective without the government's help, and vice versa.

For our part, SIFMA has recently undertaken a five-part effort to address cybersecurity threats and related risks to its membership of banks, broker-dealers and asset managers and the financial services industry at large. We have established a task force of 30 firms representing a broad cross section of the industry who are engaged in this work to ensure the unique interests and needs of institutions of all shapes and sizes are addressed. The ultimate goal of these five initiatives is to better identify the vulnerabilities for a cyber attack and prepare individual firms and the broader sector to defend themselves, thereby enhancing protections for the capital markets and the millions of Americans who use financial services every day.

Standards

Effective cybersecurity regulatory guidance is critical for both the financial services sector and the other critical infrastructure sectors we rely on. SIFMA commends the various regulatory agencies for conducting a review of their cybersecurity policies, regulations, and guidance and conducting surveys and sweeps of the firms that they cover with the goal of strengthening the defense and response of firms to cyber attacks and to better understand the investments that firms have already made to address this risk.

In addition to the reviews being conducted, we have suggested, via our published Principles for Effective Cybersecurity Regulatory Guidance,[2] that regulations be harmonized across agencies for greater effectiveness. Industry looks to the government to help identify uniform standards, promote accountability across the entire critical infrastructure, and provide access to essential information and SIFMA urges policymakers to consider how best to incorporate the principles into their respective regulatory initiatives.

SIFMA's principles build upon the highly valuable NIST Cybersecurity Framework—an initiative which we contributed much time and energy to and after its release, have sought out opportunities

[2] SIFMA Principles for Effective Cybersecurity Regulatory Guidance: http://www.sifma.org/issues/item.aspx?id=8589951691

to promote its use within the sector by mapping existing compliance requirements so firms can see where they could not only achieve risk management benefits but compliance benefits as well.

Likewise, government depends upon industry to implement regulation or guidance and collaborate on identifying risks and providing effective solutions to those highlighted areas. An illustrative example of this industry collaboration is how we are addressing the management of third party relationships and the cybersecurity risks that arise from them. A standardized set of controls and a process for implementing and evaluating those controls by third parties would foster greater transparency and confidence in a critical component of our overall ecosystem. Today, regulated utilities and service providers must answer various firms' non-standard requests for information on their cybersecurity practices and other critical areas. This information is important to all stakeholders, but is presently handled via a bespoke approach for vetting and auditing that is focused on data collection vs. active risk management. A consortium of 8 banks, 10 exchanges/utilities, and 4 audit firms is working towards streamlining the data collection process by building upon the AICPA SOC-2 criteria, the NIST Cybersecurity Framework and the specific requirements of the industry to create a control framework that is easier to execute, more comprehensive and increases the level of assurance that firms have in their thirds party providers.

Improving Resiliency in the Markets

Additionally, SIFMA assembled a working group to develop a diagnostic on the U.S. equity and Treasury markets. After mapping process flows within the markets, a workshop was held during which a set of 10 diverse cyber-risk scenarios were applied to the markets and a number of potential risks or vulnerabilities were identified. These results are being addressed via a number of public and private sector working groups. At a high level, the most important cybersecurity issues identified by the working group were the need for destructive malware defense and analysis capabilities, the development of cybersecurity standards for third party providers and the need for improved incident response coordination.

Incident Response

SIFMA's members refined the industry's crisis incident response plans to ensure that it is well tested and recognizes the appropriate role of our government partners. Building off the after-action reports and lessons learned from the cyber exercise "Quantum Dawn 2" and from our experience in

Superstorm Sandy, SIFMA developed and documented the protocols and process to create an industry consensus recommendation to respond to a systemic incident within the Equity and Fixed Income markets. To enable this process, SIFMA created two new market response committees covering these two markets, which will facilitate discussion and decision-making in the event of a crisis. In order to develop a comprehensive review and recommendation for an incident, these committees include SIFMA member firms, exchanges and utilities, securities regulators and Treasury as our sector specific agency. On October 24, 2014, SIFMA conducted a test of the process with extensive participation by both committees, resulting in an after-action report that will drive additional improvements. In support of the Financial Services Sector Coordinating Council (FSSCC), SIFMA launched a multi-faceted approach to engaging the government in order to facilitate a common understanding of how the capital markets will be supported in the event of an attack and what mechanisms and capabilities are available for defending the markets, and in turn investors, while re-establishing public confidence in the recovery.

This dialogue has evolved into a joint exercise program composed of quarterly table top exercises for both public and private sector firms and agencies to discuss the specific capabilities and response processes that would be executed in the event of a successful cyber attack against the financial industry. These exercises produce after action reports which are then used by the sector and Treasury to drive improvement and ensure we are prepared as an industry and nation to respond.

Insider Threat

As we have learned from recent events, the threat of breach and unauthorized disclosure can appear from both external and internal sources and both need to be actively addressed and monitored. Building upon a proactive approach to cybersecurity, SIFMA developed a set of best practices from a number of public and private sector sources to assist firms in the development of their own insider threat mitigation programs. This best practices guide provides context, considerations, and a method for implementation of an insider threat program that aligns with the NIST Cybersecurity Framework to facilitate integration into firms' cybersecurity programs and allow synergies to be leveraged as many risks overlap.

Information Sharing

SIFMA has worked to deepen our members' engagement with the Financial Services Information Sharing and Analysis Center (FS-ISAC) and by experimenting with unique ways to drive membership. The FS-ISAC is the global financial industry's go-to resource for cyber and physical threat intelligence and a key operational component of the sector's defense. Its role is so central that on November 3, 2014, the Federal Financial Institutions Examination Council (FFIEC) recommended that financial institutions should join sector-wide information sharing organizations like the FS-ISAC. The FFIEC noted that "participating in information-sharing forums is an important element of an institution's risk management processes and its ability to identify, respond to, and mitigate cybersecurity threats and incidents." In line with this recommendation, SIFMA has funded a one year membership for 181 SIFMA members in the small firm category in order to achieve a near 100% membership overlap with FS-ISAC.

In addition to promoting information sharing, we have also sought ways to increase the level of cyber defense and readiness for small firms, by publishing a cybersecurity guidebook informed by best practices at larger institutions and government partners centered on the NIST Cybersecurity Framework. Looking into the future, SIFMA and its members are leaders in both the development and support of Soltra Edge, a software solution from DTCC and FS-ISAC that is designed to facilitate the collection of cyber threat intelligence from various sources, convert it into an industry standard language and provide timely information on which users can decide to take action to better protect their company. SIFMA sees Soltra as a significant step forward in sharing threat information at machine speeds within the sector and ultimately with other sectors, third parties and agencies of the US Government. This is another great example of the sector partnering and innovating at a rapid pace to address the cybersecurity risks we face and increase the costs for attackers.

Overall, there has been a marked improvement in information sharing between the financial sector and Law Enforcement, the Departments of the Treasury, and the Department of Homeland Security. Department of Justice anti-trust clarifications and improved turnaround time on security clearance approval requests have also better equipped information security officers with actionable information. A few aspects of the industry-wide cybersecurity effort, however, would particularly benefit from greater U.S. government involvement:

(i) More clarity on how roles of various USG authorities match up with specific aspects of cybersecurity

(ii) Higher quality and increased frequency of classified briefings to sector

(iii) Accelerated timing of security automation objectives

(iv) Accelerated timing of cybersecurity R&D initiatives

(v) Focus on attracting a wider cybersecurity talent pool / work force to address shortage

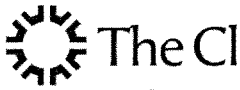
Furthermore, as I mentioned, there is a need for Congress to continue their productive engagement in this effort to improve our cybersecurity and the best place to focus is taking up and passing S. 754, the Cybersecurity Information Sharing Act (CISA) of 2014, which received large bipartisan support in the Senate Intelligence Committee this past March. While the House has done its part to move the ball forward, the threat our economy faces from cyber attacks is real and information sharing legislation will help the financial services industry to better protect our systems and data as well as the privacy of our customers. The financial services sector cannot wait for the next attack to get a bill to the President's desk and so SIFMA calls on the Senate to act on CISA and for the House and Senate to reach quick agreement through a conference. Congress must remain vigilant and proactive and provide the private sector with laws that will enable us to better protect ourselves and collaborate with our government partners.

Conclusion

Neither the industry nor the government can prevent or prepare for cyber threats on their own. SIFMA believes that a dynamic and collaborative partnership between the industry and government is the most effective path forward to accomplishing this goal. Among other areas for collaboration, government participation in industry exercises is critical to gain a better understanding of our collective capabilities in the event of a crisis. For Quantum Dawn 3 (QD3), we are currently planning for a major industry-wide exercise in Q3 2015. QD3 will build upon the breadth and success of QD2 and continue to focus on an attack on the US equity market that has a systemic impact. The exercise will include participants from the public and private sector and focus on how we collaborate during a crisis to maintain operations in the face of an attack.

As an industry, we have made cybersecurity a top priority. It is an issue my member companies worry about every day. SIFMA has brought together experts from across the public and private sectors to better understand the risks involved in a cyber attack and develop best practices to be better prepared to thwart an attack, but to be effective, we must work closely with the federal government to strengthen our partnership, protect our economy and the millions of Americans who place their confidence in the financial markets each and every day.

###



Testimony of Russ Fitzgibbons, Executive Vice President and Chief Risk Officer
The Clearing House Payments Company
Before the House Financial Services Committee
Subcommittee on Financial Institutions and Consumer Credit
"Protecting Critical Infrastructure: How the Financial Sector Addresses Cyber Threats"
May 19, 2015

Good afternoon Chairman Neugebauer, Ranking Member Clay, and members of the Subcommittee. My name is Russ Fitzgibbons and I am the Executive Vice President and Chief Risk Officer of The Clearing House Payments Company L.L.C. (The Clearing House). As Chief Risk Officer, I am responsible for enterprise risk management, information security, and business continuity. I also serve as the current Chair of the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC). I appreciate the opportunity to appear before you today to discuss issues that are critical to all Americans—the protection of our payments systems against cyber threats.

The Clearing House is the nation's oldest banking association and payments company, founded in 1853 and owned by twenty-six banks. Our mission is to ensure the safety, soundness, and efficiency of the payments system in particular, and to enhance financial stability more generally. The Clearing House provides payment, clearing, and settlement services to our owner banks and other financial institutions, clearing and settling nearly $2 trillion daily. The Clearing House's owner banks collectively hold over 55% of the nation's deposits; issue over 40% of debit cards; and issue over 70% of Visa and MasterCard-branded cards. The Clearing House also engages in payments technology and payments systems security advocacy.

The Clearing House operates the Clearing House Inter-bank Payments System (CHIPS) and the Automated Clearing House (ACH). We are the only private-sector ACH operator in the country, processing approximately 50% of all commercial ACH volume in the United States through our networks. CHIPS is the largest private-sector U.S.-dollar

funds transfer system in the world, clearing and settling an average of $1.5 trillion in payments—both domestic and cross-border—daily.

The Clearing House also seeks to leverage its core capabilities to enable innovation across the sector. We regularly work with our owner banks and others to develop next generation payment systems—with the same safety and soundness principles that have always underpinned our core systems. For example, we are currently working to deploy a tokenization platform to enhance the security of credit and debit card transactions, including those made online, and developing a real-time payment system.

Because of the volume and importance of the financial transactions enabled by The Clearing House's systems, robust protection of those systems from cyber threats is essential.

Cyber threats to banking infrastructure have become more frequent and more sophisticated in recent years. The criminal organizations and other groups launching these threats are constantly innovating, and we need to be at least as agile as they are in defending ourselves.[1]

I will divide the remainder of my remarks into three areas:

A. **Financial Sector Efforts:** Ways in which financial institutions such as The Clearing House are working to defend ourselves against cyber threats, including through technological innovations and cooperation within the private sector;
B. **Strengthened Collaboration Between the Private Sector and Government:** The crucial role that strengthening our partnerships with government can and must play in further enhancing the security and resilience of our payments and financial systems;
C. **Legislative Assistance:** Areas where action by Congress could help both the financial services sector and our government partners work even more effectively to advance our common goal of strengthening the financial sector's resilience in the face of cyber attacks.

A. Financial Sector Efforts

Let me begin by discussing some of the ways in which financial institutions work to defend themselves and their customers against cyber threats, both on their own and frequently in collaboration with other financial services firms and industry organizations.

---

[1] See, e.g., Cedarbaum and Reilly, Cybersecurity Collaboration: Routes to Stronger Defenses, Banking Perspective (Q1 2015) at 68-69.

First, as you know, financial institutions have been subject to the requirements of the Gramm-Leach-Bliley Act (GLBA) for roughly a decade and a half. The GLBA requires financial institutions to adopt "administrative, technical, and physical safeguards" that help ensure the "security and confidentiality of customer records and information," "protect against any anticipated threats or hazards to the security or integrity of such records," and "protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any customer."[2]

Financial institutions are also subject to other special legal and regulatory requirements such as those promulgated by the federal financial regulatory agencies of the Federal Financial Institutions Examination Council (FFIEC). For example, the FFIEC has issued "Interagency Guidelines Establishing Information Security Standards" (Interagency Guidelines), which direct financial institutions to implement "a comprehensive written information security program." Financial institutions' information security programs must include five basic components, including oversight of service providers. Pursuant to these requirements, The Clearing House's data security practices are subject to regular examination and supervision through the FFIEC's Multi-Regional Data Processing Servicer Program (MDPS).

As threats to our payments infrastructure evolve, so too do our defenses. Technological innovation is an important weapon in our arsenal. One example of innovation that is being readied for deployment is Secure Token Exchange, a new platform of The Clearing House which replaces account numbers with randomly-generated temporary numbers during processing. With Secure Token Exchange, the customer's actual account information is not transmitted outside of banks and their service companies. This type of anonymization provides a layer of security for customers, merchants, and banks while preserving the current customer experience. Secure Token Exchange reduces the risk of cyber criminals being able to gain access to customers' financial information because the information exists only behind the firewalls of highly regulated and supervised financial institutions and their service companies. Over the coming months and years we will be transitioning credit and debit card payment transactions to Secure Token Exchange. We believe this model is scalable to other facets of the payments system, including ACH transactions and the real-time payment system currently under development by The Clearing House.

Effective cybersecurity requires more than technological innovation and sophistication. It requires organizational dexterity and agility as well. Like many other financial institutions, The Clearing House has made training and exercises an increasingly important component of our cybersecurity efforts. Just to give one example, the Financial

[2] 15 U.S.C. § 6801(b).

Services Information Sharing and Analysis Center (FS-ISAC), has for several years held an annual two-day simulation known as The Cyber Attack Against Payments Processes (CAAPP) designed to enable companies such as The Clearing House to put their cyber defense processes to the test and thus identify areas for improvement.

Effective cybersecurity also requires awareness and early warning of potential threats and risks. In part, we do this by participation in information-sharing programs. Our primary mechanism is via the FS-ISAC, which has over 5,000 member organizations and has become an operational information-sharing model for other sectors. It has found a good balance of member-to-member and sector-wide sharing of threat analysis information, vulnerability data and indicators of potential problems. Of particular note, FS-ISAC enables institutions to share information anonymously.

FS-ISAC members, which range from small community banks and credit unions to some of the largest financial institutions in the world, make contributions to the information-sharing effort commensurate with their resources and capabilities. Large bank members, which by and large have substantially greater resources to devote to threat intelligence collection and other information-gathering efforts, play a particularly important role, and their contributions benefit the entire sector, as they are disseminated through the FS-ISAC platform.

There are several types of information that are shared with high frequency, including:

- Identity of servers used by malicious cyber actors and the routes over the internet they use to deliver their attacks;
- Malware and other threat signatures, which are used for scanning networks to detect the presence of threats;
- Attack vectors, which are paths for gaining access to a system; and
- Situational awareness intelligence.

As the volume of threat activity has grown, the need for effective automated information-sharing has become crucial to ensuring that financial companies can respond rapidly to the shifting threat environment. Enabling efficient and time-sensitive information-sharing is a priority at the highest levels of our member banks, with two CEO's taking the industry lead to ensure that this effort is fully realized.

Through FS-ISAC and Depository Trust & Clearing Corporation (DTCC), the sector recently deployed a more effective platform for real-time automated sharing of cyber threat information called Soltra Edge. Utilization and integration of Soltra Edge across the sector's infrastructure are expected to grow significantly over the next few years.

Cross-sector information-sharing can also make an important contribution to cybersecurity. Thus, the FS-ISAC and others have been working with other sectors (e.g., energy, telecommunications, retail and legal sectors) to join forces in information-sharing efforts.

B. Strengthened Collaboration Between the Private Sector and Government

In response to the growing cyber threats we face, financial institutions have dramatically increased their own investments in cybersecurity defensive measures. But comprehensive cybersecurity requires that the federal government use its authority and capabilities to proactively mitigate threats and work with the financial community to employ defensive measures. Addressing the cybersecurity challenge requires a team effort. We must be data driven in our assessment of threats and risks and prioritize accordingly. We must also maintain and enhance the collaboration and teamwork that happens in the sector today. Our efforts must scale at the same pace or faster than the risks our networks face.

Through FS-ISAC and other organizations, we coordinate closely with the National Infrastructure Coordinating Center (NICC), the Department of Homeland Security operations center that maintains awareness of critical infrastructure for the federal government and law enforcement agencies. We actively participate in the Financial Services Sector Coordinating Council for Critical Infrastructure Protection and Homeland Security (FSSCC), of which, as I previously mentioned, I am currently the Chair. We also work closely with the Treasury Department's Office for Critical Infrastructure Protection and Compliance and its Cyber Intelligence Group.

In my estimation, the goodwill between government partners and the financial sector is at an all-time high. There is an increased sense of urgency, the operations tempo is improving, and the depth of information shared is much better than in the past. One notable example is the effort to streamline the process for financial companies to request technical assistance from the government in responding to cyber threats. This joint effort between the Securities Industry and Financial Markets Association (SIFMA), other trade associations, various government agencies, and several financial firms will help to improve collaboration between the financial sector and our government counterparts during cyber incidents. This effort helps the sector become more resilient.

While the financial services sector has made considerable strides in its sharing within the sector and with our government partners, there are still areas for improvement. Companies in the financial sector share information quite extensively with the government, and the flow of information from government agencies to the private sector has increased significantly. But we have lots of opportunity to improve our ability to support our cyber first responders, defend critical infrastructure, and protect our stakeholders. The

Administration has issued two executive orders designed to improve the government's sharing of information with the private sector, and there have been resulting improvements. However, more work needs to be done on the analysis and contextualization of threat information, and government agencies need to continue increasing their prioritization and allocation of resources for declassifying information that pertains to network defense.

We also need more affirmative efforts by the government to defend the private sector against cyber threats, especially those emanating from abroad. To the extent lack of certainty about the government's legal authority to act has hampered government action, those authorities should be clarified. A good example of this is included in the Administration's cyber legislation proposal. "One powerful tool that the [Justice D]epartment has used to disrupt botnets and free victim computers from criminal malware," the head of the Justice Department's Criminal Division has noted, "is the civil injunction process."[3] "The problem is that current law only permits courts to consider injunctions for limited crimes."[4] The Administration's current legislative proposal would add operation of a botnet to the list of offenses eligible for injunctive relief, thus clarifying the government's ability to use civil injunctions to go after cyber criminals and shut down botnets, which are often used as platforms for attacks on financial services companies.

C. Legislative Assistance

We also believe that Congress has a role to play in promoting greater and more effective cybersecurity. Information-sharing efforts have greatly improved in recent years and already make an important contribution to the financial sector's cybersecurity. But concerns about various forms of liability exposure resulting from information-sharing continue to make information-sharing less vigorous than it should be and thus weaken our sector's cybersecurity capabilities. The Justice Department's recent white papers on antitrust and Stored Communications Act issues have helped address some of those concerns. Others, however, remain. Thus, action by Congress to pass comprehensive cyber threat information-sharing legislation with protections against liability for companies that collect and share in accordance with the law is essential.

We agree with our financial services counterparts and support both bills passed by the House in April: the National Cybersecurity Protection Advancement Act of 2015 (H.R. 1731), and the Protecting Cyber Networks Act (H.R. 1560). We also support the leading Senate bill, the Cybersecurity Information Sharing Act of 2015 (S. 754). However Congress

---

[3] Assistant Attorney General Leslie R. Caldwell, Assuring Authority for Courts to Shut Down Botnets (Mar. 11, 2015), available at http://www.justice.gov/opa/blog/assuring-authority-courts-shut-down-botnets.

[4] *Id.*

decides to move forward with these bills, we believe that any final legislation that is sent to the President must accomplish the following:

- Facilitate real-time sharing to enable institutions and governments to act quickly;
- Provide liability protection for cyber threat sharing within the private sector and between the private sector and the government;
- Provide liability protection for system monitoring and other essential self-defense measures companies take on their own networks;
- Provide protection from disclosure of information shared with the government through the Freedom of Information Act (FOIA) and limit the use of such information to cybersecurity purposes;
- Facilitate the appropriate declassification of information by the intelligence agencies and expedite issuance of clearances to private sector individuals;
- Include appropriate privacy protections, especially for personally identifiable information (PII); and
- Clarify the government's authorities to take action to defend the private sector.

Thank you for your attention to this critically important issue and for the opportunity to testify today. I look forward to answering any questions you may have.

Financial Services Sector Coordinating Council
for Critical Infrastructure Protection and Homeland Security

Testimony of

Gregory T. Garcia

On Behalf of the

Financial Services Sector Coordinating Council

On

"Protecting Critical Infrastructure: How the Financial Sector Addresses Cyber Threats"

Before the

U.S. House of Representatives
Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit

May 19, 2015

Chairman Neugebauer, Ranking Member Clay, and Members of the Subcommittee, thank you for this opportunity to address the Subcommittee about how the financial sector addresses cyber threats.

My name is Greg Garcia. I am the Executive Director of the Financial Services Sector Coordinating Council (FSSCC). Established in 2002, FSSCC involves 65 of the largest financial firms and industry associations representing clearinghouses, commercial banks, credit card networks; credit rating agencies; exchanges; electronic communication networks; financial advisory services; insurance companies; financial utilities; government-sponsored enterprises; investment banks; merchant and retail banks; and electronic payment firms. This community shares responsibility and commitment to the protection of our sector that is commensurate with their substantial importance to the resilience of the national and global economy.

The FSSCC was established in accordance with the critical infrastructure protection framework promulgated first in Presidential Decision Directive (PDD) 63 in 1998, which was superseded in 2003 by Homeland Security Presidential Directive 7 and in 2013 by Presidential Policy Directive 21.

As with many industry associations, its governing structure includes a rotating chairmanship and an executive committee, with numerous outcome-oriented working groups focused on specific deliverables to achieve the organization's objectives. The current chairman, serving the first year of his two year term, is Russell Fitzgibbons, the Chief Risk Officer and Executive Vice President of The Clearing House.

Today I will discuss an overview of the cyber threats faced by the financial sector, and how it is organized under regulatory and partnership frameworks to manage cyber risk.

PROFILE OF THE FINANCIAL SECTOR AND ITS STATUS AS CRITICAL INFRASTRUCTURE

Congress and the Administration have defined "critical infrastructure" as "the assets, systems, and networks, whether physical or virtual, so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."

Section 9 of Executive Order 13636, issued in 2013 requires that DHS identify critical infrastructure against which a cybersecurity incident could result in catastrophic regional or national effects on public health or safety, economic security, or national security. The primary purpose of this process is to improve understanding of national and regional cyber dependencies and consequences across critical infrastructure, inform planning and program development for federal critical infrastructure security and resilience programs, and motivate identified critical infrastructure owners and operators to maintain robust cyber risk management programs.

Collectively, the organizations that make up the financial services sector are connected through a network of electronic systems with many entry points, and most of the sector's key services are provided through or conducted on information and communications technology platforms, making cybersecurity of paramount importance to the sector. A successful cybersecurity or physical attack on these systems could have significant impacts on the global economy and the nation.

For example, malicious cyber actors with increasing sophistication and persistence continue to target the financial services sector. These actors vary considerably in terms of motivation and capability, from nation states conducting corporate espionage to advanced cyber criminals seeking to steal money, to hacktivists intent on making political statements. Many cybersecurity incidents, regardless of their original motive, have the potential to disrupt critical systems, even inadvertently.

In order to maintain a strong risk management partnership against potential high-impact cyber events, the Treasury Department, financial regulators, the Department of Homeland Security, and law enforcement and other government partners coordinate regularly with financial institutions to identify critical systems, infrastructure, operations and institutions, as well as current and emerging threats to those systems, in order to develop appropriate security and resilience strategies.

FSSCC MISSION

The mission of the FSSCC is to strengthen the resiliency of the financial services sector against attacks and other threats to the nation's critical infrastructure by proactively identifying threats and promoting protection, driving preparedness, collaborating with the federal government, and coordinating crisis response for the benefit of the financial services sector, consumers and the nation. During the past decade, this strategic partnership has continued to grow, in terms of the size and commitment of its membership and the breadth of issues it addresses.

In simplest terms, members of the FSSCC assess security and resiliency trends and policy developments affecting our critical financial infrastructure, and coordinate among ourselves and with our partners in government and other sectors to develop a consolidated point of view and coherent strategy for dealing with those issues.

Accordingly, our sector's primary objectives are to:

- Implement and maintain structured routines for sharing timely and actionable information related to cyber and physical threats and vulnerabilities among firms, across sectors of industry, and between the private sector and government.
- Improve risk management capabilities and the security posture of firms across the financial sector and the service providers they rely on by encouraging the development and use of common approaches and best practices.
- Collaborate with homeland security, law enforcement and intelligence communities, financial regulatory authorities, other industry sectors, and international partners to respond to and recover from significant incidents.
- Discuss policy and regulatory initiatives that advance infrastructure resiliency and security priorities through robust coordination between government and industry.

We have learned that a strong risk management strategy for cyber and physical protection involves participating in communities of trust that share information about threats, vulnerabilities, and incidents affecting those communities. That strategy is based on the simple concepts of strength in numbers, the neighborhood watch, and shared situational awareness.

To achieve this goal, public and private sector partners exchange data and contextual information about specific incidents and longer term trends and developments. Sharing this information helps to prevent

incidents from occurring and to reduce the risk of a successful incident at one firm later impacting another. These efforts increasingly focus on including smaller firms and include international partners.

Together we are undertaking or have accomplished numerous initiatives to:

- Improve information sharing content and procedures between government and the sector;
- Conduct joint exercises to test our communications, response and resiliency protocols during incident scenarios affecting different segments of the financial system;
- Maintain an "All Hazards Crisis Response Playbook" and within it a "Cyber Response Coordination Guide" that leads incident responders and executive decision makers through decision and action processes based on identified impacts and severity of incidents;
- Prioritize critical infrastructure protection research and development (R&D) funding needs
- Engage with other critical sectors and international partners to understand and leverage our interdependencies;
- Advocate broad adoption of the National Institute of Standards and Technology (NIST) Cybersecurity Framework, including among small and mid-sized financial institutions across the country;
- Develop best practices guidance for operational risk issues involving third party risk, supply chain, and cyber insurance strategies; and
- Create financial services sector-owned, operated and governed .BANK and .INSURANCE top-level internet domains. The .BANK and .INSURANCE domains have robust operational standards including: eligibility requirements; verification; name selection standards; and security-focused technical requirements such as Domain Name System Security Extensions (DNSSEC); encryption standards; email authentication requirements designed to reduce phishing and spoofing activities; and more.

At the same time, understanding the sector's dependencies on the delivery of services from other key sectors such as communications, energy and information technology is necessary for better understanding threats and assuring rapid recovery and business continuity planning against disruption of critical financial functions, regardless of the cause.

FS-ISAC INFORMATION SHARING PROGRAMS AND OPERATIONS

For the financial sector, the primary community of trust for critical financial infrastructure protection is the Financial Services Information Sharing and Analysis Center, or FS-ISAC, which is the tactical and operational member organization that informs the FSSCC's strategic policy mission.

The FS-ISAC was formed in 1999 in response to the 1998 PDD 63, which called for the public and private sectors to work together to address physical and cyber threats to the nation's critical infrastructures. This role was reinforced after 9/11 and continues to strengthen to address evolving threats to critical infrastructure.

The FS-ISAC is a 501(c)6 nonprofit organization and is funded entirely by its member firms and sponsors. In 2004, there were 68 members, primarily larger financial services firms. Since that time, the membership has expanded to more than 5000 organizations including commercial banks and credit unions of all sizes, brokerage firms, insurance companies, data security payments processors, and 24

trade associations representing virtually all of the U.S. financial services sector. Most recently, there has been a significant increase in the number of small and medium sized entities that have joined FS-ISAC.

Since its founding, the FS-ISAC's operations and culture of trusted collaboration have evolved into what we believe is a successful model for how other industry sectors can organize themselves around this security imperative. The overall objective of the FS-ISAC is to protect the financial services sector against cyber and physical threats and risk. It acts as a trusted third party that facilitates sharing of actionable threat, vulnerability and incident information in a non-attributable and trusted manner among members, the sector, and its industry and government partners, ultimately benefiting the nation.

FS-ISAC information sharing activities include:

- Delivery of timely, relevant and actionable cyber and physical email alerts from various sources distributed through the FS-ISAC Security Operations Center (SOC);
- An anonymous online submission capability to facilitate member sharing of threat, vulnerability, incident information and best practices in a non-attributable and trusted manner;
- Support for attributable threat information exchange by various special interest groups including the FSSCC, the FS-ISAC Threat Intelligence Committee, the Payment Processors Information Sharing Council (PPISC), the Clearing House and Exchange Forum (CHEF), the Business Resilience Committee, and the Payments Risk Council;
- Bi-weekly threat information sharing calls for members and invited security/risk experts to discuss the latest threats, vulnerabilities and incidents affecting the sector;
- Emergency threat or incident notifications to all members using the Critical Infrastructure Notification System (CINS); and
- Participation in various cyber exercises such as those conducted by DHS (Cyber Storm I, II, and III) and support for FSSCC exercises such as the Hamilton series, CyberFIRE and Quantum Dawn.

FINANCIAL SECTOR PARTNERSHIPS

The financial sector works closely with various government agencies including the Department of Treasury, which leads the Finance and Banking Information Infrastructure Committee (FBIIC); DHS; Federal Financial Institutions Examination Council (FFIEC) regulatory agencies; United States Secret Service; Federal Bureau of Investigation (FBI); the intelligence community; and state and local governments.

In addition to our close working relationship with the Treasury Department and financial regulatory agencies, financial sector stakeholders participate in a variety of strategic and information sharing programs operated by DHS. For example:

- The financial sector and Treasury Department maintain a physical presence, cleared at the Top Secret / Sensitive Compartmented Information (TS/SCI) level, within the DHS National Cybersecurity and Communications Integration Center (NCCIC), which serves as a hub for sharing information related to cybersecurity and communications incidents across sectors, among other roles and responsibilities.
- Supplementing our information sharing engagement within NCCIC is the DHS Cyber Information Sharing and Collaboration Program (CISCP) which enables collaborative threat analysis between

industry and government in an operational and trusted environment that speeds time to response.

- Also useful to the financial sector, particularly smaller community institutions, is the Critical Infrastructure Cyber Community (C^3, or "C-Cubed") Voluntary Program, which supplements the NIST Cyber Security Framework, and provides guidance on how institutions can improve their cyber risk management programs, regardless of size and sophistication.
- The Office of Cyber & Infrastructure Analysis helps critical sectors evaluate cross sector interdependencies with risk and threat assessments, and is currently undertaking an interdependency assessment between financial services and telecommunications infrastructure in the Chicago area.
- The financial sector has developed an R&D agenda highlighting the priority R&D initiatives we believe will enhance protection of our critical financial infrastructure, and we have consulted with the DHS Science and Technology Directorate to help inform their funding priorities.
- The sector also works closely with the National Infrastructure Coordinating Center (NICC), the dedicated 24/7 coordination and information sharing operations center that maintains situational awareness of the nation's critical infrastructure for the federal government.
- Most recently, the financial sector has begun planning and executing a series of sector-wide cyber exercises that test our ability to share information and respond to critical incidents collaboratively with our government partners. The DHS NCCIC management and operations team has been an important partner in this process, as have the Treasury Department and other key government stakeholders, lending their expertise and resources toward developing the scenarios and supporting the execution and after-action reports of the exercises.
- Through the promulgation of DHS-funded open specifications for automated threat information sharing, the FS-ISAC has developed a capability that is widely used by the financial sector and other sectors. Known as Soltra Edge, this tool automates threat sharing and analysis and speeds time to decision and mitigation from days to hours and minutes.
- Finally, the FS-ISAC and FSSCC have worked closely with government partners to obtain security clearances for key financial services sector personnel. These clearances have been used to brief the sector on new information security threats and have provided useful information for the sector to implement effective risk controls to combat these threats.

AUTOMATED THREAT INFORMATION SHARING

The sector continues to make significant progress toward increasing the speed and reliability of its information sharing efforts through expanded use of DHS-funded open specifications, including Structured Threat Information eXchange (STIX™) and Trusted Automated eXchange of Indicator Information (TAXII™).

Late last year, the financial sector announced the "Soltra Edge" automated threat capability, which is the result of a joint venture of the FS-ISAC and the Depository Trust and Clearing Corporation (DTCC). This capability addresses a fundamental challenge in our information sharing environment: typically the time associated with chasing down any specific threat indicator is substantial. The challenge has been to help our industry increase the speed, scale and accuracy of information sharing and accelerate time to resolution.

The Soltra Edge tool reduces a huge burden of work for both large and small financial organizations, including those that rely on third parties for monitoring and incident response. It is designed for use by many parts of the critical infrastructure ecosystem, including the financial services sector; the healthcare sector; the energy sectors; transportation sectors; other ISACs; national and regional CERTs (Computer Emergency Response Teams); and vendors and services providers that serve these sectors.

Key goals of Soltra-Edge are to:

- Deliver an industry-created utility to automate threat intelligence sharing
- Reduce response time from days/weeks/months to seconds/minutes
- Deliver 10 times reduction in effort and cost to respond
- Operate on an at-cost model over open standards (STIX, TAXII)
- Leverage DTCC scalability; FS-ISAC community and best practices
- Provide a platform that can be extended to all sizes of financial services firms, other ISACs and industries
- Enable integration with vendor solutions (firewalls, intrusion detection, anti-virus, threat intelligence, etc.)

With these advancements, one organization's incident becomes everyone's defense at machine speed. We expect this automated solution to be a "go-to" resource to speed incident response across thousands of organizations in many countries within the next few years.

REGULATORY INTERESTS

The financial sector is often credited for having developed a "mature" cyber security risk management posture. This is due in part to the fact that financial services is a heavily regulated industry, and also to the overarching imperative that our business models, consumer confidence and the stability of the financial system and the global economy are dependent upon a secure and resilient infrastructure.

As just one example, Title V of the Gramm-Leach-Bliley Act (GLBA) requires banks to develop and maintain an information security program, and implement a "risk-based" response program to address instances of unauthorized access to customer information systems.

At a minimum, a response program must:

- Assess the nature and scope of any security incident and identify what customer information systems and customer information may have been accessed or misused;
- Notify the institution's primary federal regulator "as soon as possible" about any threats "to sensitive customer information."
- Notify appropriate law enforcement authorities and file Suspicious Activity Reports in situations involving federal criminal violations requiring immediate attention;
- Take appropriate steps to contain the incident to prevent further unauthorized access to or use of customer information, and
- Notify customers "as soon as possible" if it is determined that misuse of customer information has occurred or is reasonably possible. Where appropriate, the notice also must include:
    - Recommendation to review account statements immediately and report suspicious activity;

- Description of fraud alerts and how to place them;
- Recommendation that the customer periodically obtain credit reports and have fraudulent information removed;
- Explanation of how to receive a free credit report; and
- Information about the FTC's identity theft guidance for consumers.

More broadly, financial sector institutions comply with varying cybersecurity requirements and guidance from many regulatory bodies:

- The Securities and Exchange Commission (SEC)
- Financial Industry Regulatory Authority (FINRA)
- The Federal Reserve System
- The Office of the Comptroller of the Currency (OCC)
- The Federal Deposit Insurance Corporation (FDIC)
- The Consumer Financial Protection Bureau (CFPB)
- The U.S. Commodity Futures Trading Commission (CFTC)
- State banking agencies
- State insurance agencies

The financial sector supports the need for regulatory guidance on effective standards of practice for cybersecurity risk management. It's a constantly moving target, and just as financial institutions need to regularly calibrate their controls to evolving threats, so do the regulatory agencies need to keep pace with new threats, new financial business process models and the necessary skill sets to evaluate the intersection of those two for security and resiliency purposes.

But as the regulatory agencies are independent, there is not sufficient coordination among them to ensure we are all aligned with unity of effort toward a common objective: financial services security and resiliency. Perhaps because of this, we have seen examples of agencies each asking their own set of cybersecurity examination questions. As a sector we would urge more uniformity among the regulatory agencies in their examination procedures and in the range of questions they ask. This process could be more efficient to allow financial institutions to focus more on securing our infrastructure and less on answering multiple questionnaires in different ways. And we are looking forward to seeing how agencies will or will not map their examination standards to the NIST Cybersecurity Framework. The Framework is an exemplary industry-government collaboration that involved extensive time, effort and resources in the development of guidance for tailored and scalable cybersecurity risk management.

Mr. Chairman and Members of the Committee, this concludes my testimony.

Testimony of

Jason Healey

Before the

United States House of Representatives

Committee on Financial Services, Subcommittee on Financial Institutions and Consumer Credit

Hearing on

"Protecting Critical Infrastructure: How the Financial Sector Addresses Cyber Threats"

19 May 2015

Chairman Neugebauer, Ranking Member Clay, and distinguished Members of the Committee, thank you for the honor of testifying before you on the finance sector's response to cyber threats.

Over the past nearly twenty years, I have been involved in cyber operations and policy in the military and Intelligence Community, the White House, and finance sector. I created the first cyber incident response capability at Goldman Sachs and was an early Vice Chairman of the Financial Services Information Sharing and Analysis Center. Now as an academic, serving both as a Senior Research Scholar at Columbia University's School of International and Public Affairs and as Senior Fellow at the Atlantic Council, I may be less involved in the day-to-day cyber tumult than my colleagues here today, but with a bit more freedom to analyze where we have come from and what might be next.

Regarding the cyber threat, it is surprising how little has changed. We've been concerned about the same basic threats – nation-states' warriors and spies, hactivists, terrorists, insiders, and criminals -- for twenty, thirty, even forty years. It has been clear that banks are in the crosshairs since at least 1994 when Vladimir Levin took Citibank for over $10 million.

But of course the massive expansion of those threats, and the myriad way come at the sector, is astounding.

Those early hacks were mostly from lone individuals or juvenile groups until a bit over a decade ago, when we saw what we call the "Rise of the Professional." In the years since, amateurs like Levin were no longer the norm, pushed aside by organized crime and nation states like Russia, Iran, and China who were increasingly swimming in the same waters.

Today, according to the Verizon Data Breach Investigations Report, the finance sector is hit mostly with web-application attacks (27% of the total attacks on the sector), such as phishing, to take over the user interface to a banking application.

Other important categories of attacks were payment-card skimmers (22%) and denial of service attacks (26%). The financial sector tended to have far lower levels of insider abuse than other sectors (only 7% of the total compared to 24% in the public sector and 37% in real estate) and strikingly low levels of cyber espionage, at under 1% of the total attacks compared to 40% in mining and about 30% for professional services and manufacturing.

AMAZING PROGRESS TO DATE

Fortunately, in the past twenty years the finance sector has led the way on many key technology innovations, such as firewalls and intrusion detection systems. At least as important have been the process innovations. After the Levin hack, Citibank created the world's first Chief Information Security Officer (CISO) position, held by our colleague Steve Katz.

Other process innovations that have made a real difference include working from a presumption of breach - assuming there is already a sophisticated heist underway and trying to find evidence; operationalizing the cyber kill chain to stop intrusions as early as possible; intelligence-driven operations; and, of course, effective information sharing.

Only one year after President Clinton called on the private critical infrastructure sectors to create Information Sharing and Analysis Centers, the finance sector had responded with the FS-ISAC which is still going strong today.

Based on my intelligence background, I formed the ISAC's Intelligence and Threat Working Group and am happy to say that under Byron Collie of Goldman Sachs, the group has blossomed beyond anything found in other sectors. The finance sector has, for example, launched the Soltra Edge platform to help standardize and automate the flow of real-time cyber threat information.

The finance sector has much else to brag about, such as .bank and .insurance as well as the Account Takeover Task Force (ATOTF) established in 2010. Another factor contributing to the relatively low rate of insider attacks against banks are the tremendous efforts taken by banks to implement effective controls – even as one of the watchers on the information security team, I knew my actions too were being watched. In fact, I have little doubt Edward Snowden would have been thwarted or arrested had he tried his shenanigans at a major bank rather than the National Security Agency.

It is true that point-of-sale attacks on credit cards have been getting worse, but more secure technologies are on the way, such as chip-and-pin or token-based systems.

Of course it is not just the financial institutions themselves that are making progress. During my time at the White House from 2003 to 2005, it was clear that the finance sector regulators were on active and that cooperation between the financial institutions and the government was exceptional, especially compared to other sectors.

Twelve years ago, the finance sector instituted one of the great critical infrastructure governance innovations. The financial institutions, industry association, and exchanges created the Financial Services Sector Coordinating Council on Critical Infrastructure Protection and Homeland Security, known as the simpler FSSCC, while the government created its counterpart, the Finance and Banking Information Infrastructure Committee. These twin pillars have been the foundation of effective information sharing and mutual trust to the extent that the Department of Homeland Security tried to copy the idea to other sectors with, it should be said, mixed results.

The "Interagency Paper on Sound Practices to Strengthen the Resilience of the U.S. Financial System" issued by the Board of Governors of the Federal Reserve in 2003 was one of those relatively simple documents that really helped shift the industry. I often tell my students that finance did resilience before it was cool.

Few remember it now, but the FS-ISAC would likely never be as strong as it is today if it hadn't received a grant twelve years ago from the Department of the Treasury. The FS-ISAC used this to recapitalize on the condition that it would provide service to all regulated American financial institutions, not just those who paid a membership fee.

Cooperation has continued to be effective, particularly through efforts like the Federal Financial Institutions Examination Council's (FFIEC) Cybersecurity and Critical Infrastructure Working Group (CCIWG) and Financial Sector Cyber Intelligence Group of 2014.

BUT WORRIES CONTINUE

The Committee need not be overly concerned about a large-scale disruptive attack taking down the finance sector. While the impacts could be terrible, these kinds of attacks are far more difficult to trigger than you may have been led to fear. Perhaps the first use ever of the term "electronic Pearl Harbor" was actually in testimony to the House Committee on Science, Space and Technology in 1991.

So even though Congress has been hearing for nearly twenty five years that a major cyber attack could cripple the United States, no major attacks have even come close.

During my work writing the first history of cyber conflict it became clear that is easy to take down a target using the Internet, but far more difficult to keep it down over time in the face of determined defenses. And as we saw after the attacks of September 11th, the finance sector can be *extremely* determined.

This should not mean the sector should rest on its successes to date. An optimist might say a digital Pearl Harbor will never come, while a pessimist will insist we're overdue. As a realist, I'd recommend work across several areas.

First, the sector should prepare not just for isolated incidents but conflict and shocks. I'm deeply worried that the finance sector will get caught up in what I believe is the most dangerous moment we've seen for cyber conflict.

From the earliest days of cyber intelligence, a rule of thumb was that "those with the capability to do us significant cyber harm lack the intent; those with the intent lack the capability." High-end adversaries simply did not launch major disruptive attacks as it frankly was not in their larger interests. Terrorists might want to cause a cyber 9/11, but haven't had the means.

But if the talks with Iran collapse, we might see a rapid spike in truly disruptive attacks by a dangerous cyber adversary, which no longer has a stake in a stable global financial system. This should not induce us to sign a deal which we may not have signed anyhow, of course, but it must be a contingency for which the sector is preparing.

Likewise, President Putin of Russia may feel that with his economic back against the wall, he would have little to lose and much to gain by throwing some just-deniable-enough cyber sand in the financial and economic gears of the West. Finance would be an obvious target for his little green bytes: mess with Russia's economy, and you'll feel pain too. He would never initiate such an attack out of the blue, but he already seems to feel he is in a conflict with us, a conflict he may see as increasingly existential.

This danger requires immediate contingency planning within the sector and with regulators and other Federal partners, along with coordination with our international partners particularly in Europe.

Second, what happened to Sony Motion Pictures last year could happen to any company in any sector. The best defended financial institutions operate under a presumption that they have already been breached, and might be able to thwart some of the worst effects. But the North Koreans have shown all of America's adversaries a new tactic, one which if used against a major bank would go far beyond cyber vandalism.

A next-generation Sony-style attack would not take down the sector as a whole, but could seriously disrupt a systemically important financial institution for days.

Last, a finance sector response will be challenged if a sector-wide emergency lasts more than a few days or weeks. Too many people who are key to the sector-wide response are also key to the response of their own financial institution. Some firms have been adding staff to give them more staying power, and a great sign of this weakness being addressed is the hiring of Greg Garcia to be the Executive Director of the FSSCC.

I suspect, though, that exercises like the Quantum Dawn series will show that there is still more to do. The sector must continue these exercises and as it is so international, the exercises must include foreign institutions and foreign regulators. The US-UK finance war game announced earlier this year is a great start.

WHAT NEXT

The best cyber regulations have not pushed security or information sharing. Rather, they have mandated transparency.

The early data-breach notification laws were true game changers and I'm pleased that Congress has been taking this topic seriously. And if a financial institution is not taking cyber risks seriously, its shareholders must be told so they can put pressure on their representatives, the board of directors.

Indeed, in this vein I believe that the Administration should do more to convince financial titans like Warren Buffett and activist institutional investors like CalPers to better understand cyber risks so they can pressure boards themselves, in their own long-term financial interest.

At least as important, the Federal government must lead from the front in three areas. The government pushes the need to share information, but too much remains government information on cyber threats remains classified. The Executive Branch has improved over the last few years, but there is much farther yet to go and the secretive national security and law enforcement agencies might need some oversight from this Committee and others for some added push.

Likewise, the Executive branch is quick to criticize others for lax security practices, even in the face of their own miserable FISMA scores.

And even though it is in the long-term interest of the United States to have a norm that financial infrastructure should be off limits to foreign attacks, the Department of Defense has not made clear statements to that effect. General Keith Alexander came very close in his

response to advance questions for his confirmation from the Senate in 2010, but Admiral Rogers did not repeat the restriction in his own response in 2014. This is likely an oversight, but it seemed to some watchers that perhaps US Cyber Command was putting finance sector targets back on the table.

This subcommittee might also usefully push the Department of Homeland Security and the Pentagon to think of a broader set of possible responses from the military to give the finance sector more staying power in a sustained conflict.

When I was working sector-wide incidents with the FS-ISAC, I can't remember pining for military cyber ninjas or wishing for the Pentagon to lay down suppressing fire. Usually, we simply needed a few more competent people who knew how to keep their heads together during a crisis, who could help wrangle the many details, tasks, sub-groups, and endless crisis teleconference calls. In short, the responses could have been far more successful not with cyber ninjas but with solid officers and NCOs ready to roll up their sleeves. We wouldn't want the sector to stumble simply for the lack of a few MOUs in place beforehand to make this possible.

Thank you for your time; this concludes my testimony.

Statement of the Robert S. Nichols
President and Chief Executive Officer, Financial Services Forum

Testimony Before the
Subcommittee on Financial Institutions and Consumer Credit
of the
House Financial Services Committee

May 19, 2015

Introduction

Chairman Neugebauer, Ranking Member Clay, thank you for the opportunity to participate in today's hearing on the threat posed by cyber attacks to our financial system.

As you mentioned, I am here as President and Chief Executive Officer of the Financial Services Forum. The Forum is a financial and economic policy organization comprising the chief executive officers of 18 of the largest and most diversified financial institutions with operations in the United States. The Forum works to promote policies that enhance savings and investment, and that ensure an open, competitive and sound global financial services marketplace.

Mounting Threat of Cyber Attack

Today's hearing is both enormously important and remarkably timely. In recent years cyber attacks have grown rapidly, both in number and level of sophistication. According to Symantec Corporation, a leading information and Internet security firm, cyber attacks around the world soared 91 percent in 2013 alone.

Just last week, the Depository Trust & Clearing Corporation, a New-York-based securities settlement and clearing firm, released its Systemic Risk Barometer for the first quarter of 2015, based on a survey of financial market participants. Asked to identify the top risks to the financial system, respondents cited cyber attack as the number one threat, with respondents specifically noting the growth in the "frequency and sophistication of cyber-attacks."

As the sophistication and frequency of attacks has increased, so have the range of culprits. Unfriendly nation-states breach systems seeking intelligence or intellectual property. So-called "hacktivists" aim to make political statements through systems disruptions. And organized crime groups, cyber gangs, and other criminals breach systems for monetary gain. A growing black market for breached data further encourages such attacks.

In some cases, the attackers appear to be parts of state-sponsored cyber-espionage efforts. It should come as no surprise that North Korea chose to target the South Korean financial system's cyber-infrastructure. Just a few days ago on May 12th, *Politico* reported that sophisticated hackers, thought to have ties to the Kremlin, used malware to launch an attack on a number of large international financial institutions. Cyber attacks on financial institutions not only threaten the security of financial information belonging to American households and

businesses, but can also, potentially, threaten financial institutions themselves, financial stability, the broader economy, and, ultimately, our national security.

Financial Industry Cyber Defense Efforts

Effectively defending against the mounting threat of cyber attack requires resources, technical sophistication, and cooperation – among financial institutions and between the financial industry, other critical infrastructure sectors, and the relevant government agencies. Large financial institutions are working hard to deliver every day on each of these critical fronts.

In the same way that community banks have the local knowledge that positions them to service their communities in unique ways, large globally active financial institutions are positioned to play a crucial role in protecting not just their banks' customer information, but the financial system as a whole.

With regard to resources and technical expertise, large financial institutions remain at the cutting edge of cyber protection and are regarded by most experts – both in the private sector and in government – as having developed and deployed some of the most sophisticated and effective defenses against cyber attacks in the corporate world.

With regard to industry cooperation and coordination, cyber security in the financial sector is a team effort – because it has to be. To be successful, the industry must invest in, and operate within, a single unified cyber security culture. And we do. Working with our colleagues across the financial sector, large institutions continuously enhance the sector's capabilities, processes and procedures, and incorporate lessons learned from real incidents and exercises.

In particular, large financial institutions are investing in ever-more robust and automated systems of threat analysis and sharing. Automated threat analysis enables the quick and reliable differentiation of lower-level problems from more serious threats, allowing our cyber defense professionals to focus on more sophisticated and malicious activity. And automated sharing enables the swift dissemination of threat information across the financial system.

In other hearings before this Committee, some witnesses have questioned whether America needs large globally active financial institutions. Mr. Chairman, the U.S. economy is the largest and most complex economy in the world, with a highly diverse range of financial product and service needs. Meeting those diverse needs requires financial institutions of all sizes and business models.

In the cyber defense arena, it is often the largest institutions that have the resources, and that are making critical investments, to combat emerging threats as they proliferate and grow in frequency and sophistication. As difficult and expensive as it is to build and maintain a robust cyber defense network, making major changes to those networks – due to forced divestitures or other major structural changes at financial institutions – would entail significant risks, including: overall network defense during and after the transition, the potential loss of top firm talent, and potential loss of intellectual property of home grown cyber security solutions.

Industry-Government Cooperation Critical

Cooperation between industry and government is also vital if the battle against mounting cyber threats is to be won. To date, cooperation with the relevant government agencies has been good, but can and must be much better. In particular, industry efforts regarding threat assessment and information sharing are constrained by lingering fear of legal liability and potential exposure, even if cyber threat information is shared in good faith and for appropriate defense purposes.

To effectively combat the mounting threat of cyber attack, financial institutions – again, widely regarded as the most sophisticated and effective defenders against cyber attacks in the corporate world – should not have to worry when sharing threat information with law enforcement, regulatory agencies, the Department of Homeland Security, or the Treasury Department. Such concerns leave financial institutions unnecessarily exposed to operational and reputational risks, undermining the cyber defense efforts in which industry and government have a pronounced mutual interest.

To encourage better cyber threat information sharing within the financial sector, and between industry and government, legislation providing sensible "Good Samaritan" protections is needed. Such legislation should:

- Facilitate real-time cyber threat information sharing to enable financial institutions and government to act quickly;
- Provide liability protection for good faith cyber threat information sharing;
- Provide targeted protections from public disclosures, such as exemptions from certain Freedom of Information Act requests;
- Facilitate appropriate declassification of pertinent government-generated cyber threat information and expedite issuance of clearances to selected and approved industry executives; and,
- Include appropriate levels of privacy protections.

With these needs in mind, the bill passed by the House on April 22nd is a major and important step forward, and will greatly facilitate industry's continued cooperation with government. We hope the Senate will soon take up its information sharing proposal to continue progress on this important issue. We urge swift movement and passage on this important legislation.

Conclusion

Chairman Neugebauer, cyber attacks on our nation's financial institutions and financial system are a regrettable fact of life in the digital age – one that can only be expected to spread and intensify in the future. Fortunately, America's financial institutions and, in particular, large financial institutions, continue to develop and deploy state-of-the-art corporate cyber defense tools, methods, and systems. But we cannot win this fight alone. For America's financial system to effectively anticipate, protect against, and respond to cyber threats, government – and industry's undeterred cooperation with government – is essential.

As financial institutions, data and information are the tools we work with and no issue is of higher priority than protecting our customers, their savings, and their financial information. Large institutions know that the bad guys are going to continue to find new and innovative ways to attack the network and systems that we fight to protect. But we will be able to be nimble in response if we can do a couple of things well:

1) Find, maintain and develop talented cyber-security experts in the financial sector;

2) Focus on good crisis management preparation and operational preparedness which increases speed to recovery; and,

3) Continue to work in partnership with the government entities and others across the financial system to share information to enhance security.

On behalf of the Financial Services Forum and its members, I commend you and Ranking Member Clay for your attention to this critical issue. We look forward to working with you to ensure that America's financial system, institutions, households, and businesses receive the protection that they need and deserve.

May 19, 2015

Cybersecurity: The Community Bank Perspective

On behalf of the more than 6,000 community banks represented by ICBA, thank you for convening today's hearing on "Protecting Critical Infrastructure: How the Financial Sector Addresses Cyber Threats." The financial services industry and community banks are on the front lines of defending against cyber threats and take their role in securing data and personal information very seriously. ICBA is pleased to take this opportunity to submit the following statement for the record which sets forth the community bank perspective on cybersecurity.

Threat Information Sharing is Critical. ICBA supports the sharing of advanced threat and attack data between federal agencies and the appropriate financial sector participants, including community banks. Community banks and their third-party service providers rely on this critical information to help them manage their cyber threats and protect their systems. ICBA strongly supports H.R. 1731 and H.R. 1560, passed by the House in April, which would provide liability protection with regard to information sharing, while balancing the need to protect privacy. These bills will help foster a more robust cyber threat information sharing ecosystem.

ICBA also supports community banks' membership and involvement with services such as the Financial Services Information Sharing and Analysis Center (FS-ISAC). The FS-ISAC is a non-profit, information-sharing forum established by financial services industry participants to facilitate the public and private sectors' sharing of physical and cyber threat and vulnerability information. ICBA also supports FS-ISAC efforts to gather complex threat information across communities, people and devices and analyze, prioritize, and route that information to users in real-time. These efforts must incorporate community banks and be cost effective for them.

All Critical Infrastructure Sectors Must Be Covered and Existing Mandates Must Be Recognized. ICBA supports the 2013 Executive Order and the NIST framework implementing it because they create a baseline to reduce cyber risk to all critical infrastructure sectors. This is a critical test for any new legislation, frameworks, or standards in the area of data security: It should extend comparable standards to all critical infrastructure sectors, including the commercial facilities sector which incorporates the retail industry and other potentially vulnerable entities. Financial institutions have long been subject to rigorous and effective data security protocols established by the Gramm-Leach-Bliley Act. Any new data security mandates must recognize the existing standards and practices community banks observe to protect the confidentiality and integrity of customer personal data as well as to mitigate cyber threats.

Regulators Should Recognize Third Party Risk. Community banks significantly rely on third-party service providers to support their systems and business activities. While community banks are diligent in their management of third-party service providers, mitigating sophisticated cyber threats to these providers can be challenging, especially when they are connected to other institutions and servicers. Regulators must be aware of the significant interconnectivity of these third-party service providers and collaborate with them in addressing cyber threats. Regulators should evaluate the concentration risks of service providers to financial institutions. In addition, the Multi-Regional Data Processing Servicer Program should be broadened to include more core, IT service providers.

ICBA Position on Recent Data Breaches

Community bankers and their customers are deeply alarmed by the wide-scale data breaches at national retail chains and other entities. These far-reaching and costly breaches have the potential to jeopardize consumers' financial integrity and confidence in the payments system.

To mitigate this risk, ICBA calls on policymakers to consider the following:

Extend Gramm-Leach-Bliley Act-Like Standards. Under current law, retailers and other parties that process or store consumer financial data are not subject to the same federal data security standards and oversight as financial institutions. Securing financial data at financial institutions is of limited value if it remains exposed at the point-of-sale and other processing points. ICBA supports subjecting these entities to Gramm-Leach-Bliley Act-like standards with similar enforcement. It is equally important that these entities provide uniform and timely notification to banks concerning the nature and scope of any breach when bank customer information may have been compromised.

A National Data Security Breach and Notification Standard is Vital. Most states have enacted laws with differing requirements for protecting customer information and giving notice in the event of a data breach. This patchwork of state laws only increases burdens and costs, fosters confusion, and ultimately is detrimental to customers. ICBA believes customer notification is appropriate to let customers take steps to protect themselves from identity theft or fraud resulting from data breaches. However, it is important that notification requirements allow financial institutions and others flexibility to determine when notice is appropriate. Overly broad notification requirements defeat the purpose of calling attention to the risks associated with a particular breach. Federal banking agencies should set the standard for financial institutions, as they currently do.

The Party that Incurs a Breach Should be Liable for Associated Costs. It is critical that the party that incurs a data breach, whether it be a retailer, financial institution, data processor or other entity, bear responsibility for the related fraud losses and costs of mitigation. Allocating financial responsibility with the party that is best positioned to secure consumer data will provide a strong incentive for it to do so effectively. Additionally, aligning incentives to maximize data security by all parties that process and/or store consumer data will make the payments system stronger over time. Payments rules should mandate merchant security provisions to further protect customer data, particularly debit and credit card information.

Data Security Act of 2015 (H.R. 2205) Strengthens Consumer Data Security

ICBA strongly supports H.R. 2205, introduced by Chairman Neugebauer and Representative Carney, which would extend Gramm-Leach-Bliley-like standards to all entities that handle sensitive consumer

data, without duplicating the standards that already apply to financial institutions. H.R. 2205 would also replace the current patchwork of state and federal regulations for data breaches with a national law that provides uniform protections across the country.

Thank you again for the opportunity to submit this statement for the record. ICBA is committed to working with this committee to address cyber threats and data breaches brought by criminal enterprises.

NAFCU
3138 10th Street North
Arlington, VA 22201-2149
703.522.4770 | 800.336.4644
F: 703.524.1082
nafcu@nafcu.org
National Association of Federal Credit Unions | www.nafcu.org

May 18, 2015

The Honorable Randy Neugebauer
Chairman
Subcommittee on Financial Institutions
and Consumer Credit
House Financial Services Committee
United States House of Representatives
Washington, D.C. 20515

The Honorable William Lacy Clay
Ranking Member
Subcommittee on Financial Institutions
and Consumer Credit
House Financial Services Committee
United States House of Representatives
Washington, D.C. 20515

Re: Tomorrow's Hearing: "Protecting Critical Infrastructure: How the Financial Sector Addresses Cyber Threats"

Dear Chairman Neugebauer and Ranking Member Clay:

On behalf of the National Association of Federal Credit Unions (NAFCU), the only trade association exclusively representing the interests of our nation's federal credit unions, I write today regarding tomorrow's hearing entitled, "Protecting Critical Infrastructure: How the Financial Sector Addresses Cyber Threats." We thank you for holding this important hearing and applaud your leadership on this matter.

As you know, the issues of cyber security and data security are intertwined. As Congress looks at cyber security issues, the need for greater data security standards for retailers must also be addressed. Consumers at risk in the wake of a data breach often rely on their credit union to help re-establish financial safety. In the process, credit unions suffer steep losses through the reissuance of cards, the charge-off of fraud, and the staff time it can take to respond to the magnitude of many of the breaches we have seen recently. Unfortunately, not all entities are held to a federal standard in protecting sensitive financial and personal information. While credit unions have been subject to federal standards on data security since the passage of *Gramm-Leach-Bliley Act* (GLBA) in 1999, the same cannot be said for our nation's retailers.

GLBA and its implementing regulations have successfully limited data breaches among financial institutions and this standard has a proven track record of success since its enactment. This record of success is why we believe any future requirements must recognize this existing national standard for financial institutions such as credit unions. One of the reasons for GLBA's success is the scalability rather than a one-size-fits-all approach. The best way to move forward and address data breaches is to create a comprehensive and similarly scalable regulatory scheme for those industries that are not already subject to oversight. At the same time, the oversight of credit unions, banks and other financial 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 functional financial institution regulators—to promulgate new, and possibly duplicative or contradictory, data security regulations for financial institutions already in compliance with GLBA.

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 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 to take appropriate steps to protect the security and confidentiality of the information.

The regulators 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 financial 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 financial institution 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.

The security guidelines direct every financial institution 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 financial institution 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 workable for the largest and smallest in the financial services arena. As you consider cyber and data security measures, it should be noted that scalability is achievable and that it is misnomer when other industries claim they cannot have a federal data safekeeping standard that could work across a sector of varying size businesses.

At a minimum, the financial institution 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; and,
- Response programs that specify actions to be taken when the financial 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.
- 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.

NAFCU recognizes that both merchants and credit unions are targets of cyberattacks and data thieves. The difference, however, is that while retailers are not covered by *any* federal laws or regulations requiring data security or breach notification, credit unions must comply with the significant data security regulations outlined above, and undergo regular examinations to ensure that these rules are followed. Furthermore, a credit union faces potential fines of up to $1 million per day for compliance violations.

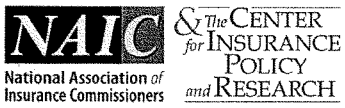
The ramifications of substandard data protections by retailers for credit unions and their members have been monumental. A February of 2015 survey of NAFCU members found that the estimated costs associated with merchant data breaches in 2014 were $226,000 on average. Of their losses, respondents expect to recoup less than 0.5%, which amounts to less than $100 on average. Despite the claims of some trade groups, the fact remains that our members are not recovering anything close to what they are spending to make their members whole after a merchant breach.

Thank you for your attention to this important matter. We look forward to tomorrow's hearing and working with the committee as you move forward in addressing data and cyber security issues. If my staff or I can be of assistance to you, or if you have any questions regarding this issue, please feel free to contact myself, or NAFCU's Director of Legislative Affairs Jillian Pevo at (703) 842-2836.

Sincerely,

Brad Thaler
Vice President of Legislative Affairs

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



May 19, 2015

Chairman Randy Neugebauer
U.S. House of Representatives
Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit
2129 Rayburn House Office Building
Washington, DC 20515

Ranking Member Wm. Lacy Clay
U.S. House of Representatives
Committee on Financial Services
Subcommittee on Financial Institutions and Consumer Credit
4340 O'Neill Federal Office Building
Washington, DC 20515

Re: Insurance Critical Infrastructure and Cyber Threats

Dear Chairman Neugebauer and Ranking Member Clay:

On behalf of the National Association of Insurance Commissioners (NAIC)[1], we write today to thank you for holding a hearing on "Protecting Critical Infrastructure: How the Financial Sector Addresses Cyber Threats." State insurance regulators take very seriously our responsibility to ensure the entities we regulate are protecting their infrastructure and the highly sensitive consumer information they retain. In this regard, we are acutely aware of the complex mission insurance regulators have of protecting consumers, laying out expectations for the insurance industry, and recognizing the economy-wide role insurers can play in driving best practices and mitigating the financial aftermath of a cyber attack.

As you know, insurance companies in the United States are subject to a stringent state-based regulatory regime designed with the primary mission of protecting policyholders. Critical infrastructure and cybersecurity issues are not new to state insurance regulators – the NAIC's *Standards for Safeguarding Consumer Information Model Regulation* sets forth standards that insurance entities must meet to be in compliance with federal and state information security laws and regulations, and the NAIC examiner handbooks for financial and market conduct exams include extensive guidance on examining controls to confirm insurance entities are taking necessary steps to protect consumers. Even when an insurer is diligent to secure its infrastructure, they may be the victim of a criminal data breach. In such an event, companies are required to inform insurance regulators in all affected states, at which point we work with law enforcement agencies and the affected company to ensure consumers are notified promptly and steps are taken to mitigate potential harm.

[1] Founded in 1871, the NAIC is the U.S. standard-setting and regulatory support organization created and governed by the chief insurance regulators from the 50 states, the District of Columbia and the five U.S. territories. Through the NAIC, state insurance regulators establish standards and best practices, conduct peer review, and coordinate their regulatory oversight. NAIC members, together with the central resources of the NAIC, form the national system of state-based insurance regulation in the U.S.

Last November, following numerous discussions about cybersecurity among our members and leadership, the NAIC established a Cybersecurity (EX) Task Force.[2] The Task Force laid out an ambitious work plan, and while much work remains, we have already made significant progress in our efforts to enhance cybersecurity protections in insurance.

Following extensive written and verbal comments by interested parties, on April 16, 2015 the Task Force approved a finalized list of 12 insurance regulatory guiding principles for cybersecurity.[3] We believe these principles create a broad framework to lay out our duties and obligations as regulators and the expectations we have for our sector. The principles will promote accountability across the entire insurance sector in the best interests of consumers. They will serve as the foundation guiding regulators who oversee the industry and provide a lens through which to assess insurance company infrastructure and efforts to protect sensitive consumer information held by insurers and producers.

The Task Force also worked with the NAIC's Property and Casualty (C) Committee to draft a Cybersecurity Insurance Coverage Supplement proposal for the annual financial statement required of insurers. This filing will provide regulators with more specific information regarding the size of the growing cyber liability market on a nationwide basis. The draft proposal was exposed for comment in March, and is currently under review by several NAIC committees. Additionally, the Task Force is working closely with the Information Technology Examination (E) Working Group to update examination protocols for financial examiners to ensure that cyber security infrastructure and controls are appropriately embedded in on-site examinations of insurers. Similar updated protocols for market conduct examiners are also under consideration.

Additional Task Force plans for the immediate future include a survey of states to assess cyber vulnerabilities, development of a "Consumer Bill of Rights" for insurance data breach victims, webinars on the benefits of information sharing, and a comprehensive review of existing cybersecurity related model laws and regulations. Furthermore, we remain committed to working alongside our Federal Colleagues as members of the Financial and Banking Information and Infrastructure Committee, chartered under the President's Working Group on Financial Markets, and the Interagency Cyber Forum for Independent and Executive Branch Regulators. We believe these forums provide a valuable opportunity to exchange regulatory best practices and strategies for promoting cyber hygiene in the sectors we oversee without a proscriptive one-size-fits-all approach.

Consumers have a right to expect that personal financial and health information entrusted to insurers and health care providers is secure. As Congress contemplates legislation in this arena, we encourage you not to limit state regulators' tools or authorities to protect policyholders. While we understand and appreciate the potential benefits of establishing common definitions and cross-sector minimum standards for data security, we remain skeptical of any efforts that involve preemption of a state's right to enact protections for its insurance consumers that go above and beyond those recommended or required by Federal law. We also are concerned with efforts to limit individual state regulators from protecting consumers in their state, regardless of where a breached insurer is domiciled. While well intentioned, such standards may actually undermine existing consumer protections, as well as inhibit future enhancements and innovation necessary for regulators and companies to adapt to evolving threats.

[2] NAIC Press Release, Nov, 19, 2015.
http://www.naic.org/Releases/2014_docs/insurance_regulators_establish_cybersecurity_task_force.htm
[3] NAIC Principles for Effective Cybersecurity: Insurance Regulatory Guidance, available at
http://www.naic.org/documents/committees_ex_cybersecurity_tf_final_principles_for_cybersecurity_guidance.pdf

The American public relies on insurance for financial peace of mind, and state insurance regulators are committed to continuing our leadership in the cybersecurity arena to maintain the trust of policyholders across the country. We commend your Committee for its attention to the issues of critical infrastructure protection and cyber threats, and look forward to working with you to design a strong data protection framework that is in the best interests of insurance consumers.

Sincerely,

Monica Lindeen
NAIC President
Montana Commissioner of
Securities and Insurance

John Huff
NAIC President-Elect
Director of Missouri's Department of Insurance,
Financial Institutions, and Professional Registration

Sharon P. Clark
NAIC Vice President
Kentucky Insurance Commissioner

Theodore K. Nickel
NAIC Secretary-Treasurer
Wisconsin Insurance Commissioner

E. Benjamin Nelson
NAIC Chief Executive Officer