December 9, 2014

The Honorable Elizabeth Warren
The Honorable Elijah Cummings

Dear Senator Warren and Ranking Member Cummings:

The Financial Services Sector Coordinating Council (FSSCC) is aware of your letter of November 18, 2014 to a select group of financial institutions related to cybersecurity, including potential breaches. We welcome your interest and commitment to improving our nation's cybersecurity and look forward to working with you toward this common goal.[1]

In your letter you ask a number of questions regarding each financial institution's cybersecurity. Given our role as the sector coordinator for financial services and the protection of critical infrastructure, we thought it would be beneficial to take this opportunity to provide an overview of the financial sector's practices, as well as to inform you of some of the initiatives that we have undertaken with our government partners to improve efforts in addressing the dynamic cybersecurity challenges facing our nation.

The FSSCC was established in 2002 and continues to serve as the coordinating body for the financial sector. Our mission is supported by Homeland Security Presidential Directive 7, which directs government agencies to identify and protect critical infrastructure. The FSSCC has 64 volunteer member associations and financial institutions representing information sharing organizations, clearinghouses, commercial banks, credit rating agencies, exchanges/electronic communication networks, financial advisory services, insurance companies, financial utilities, government-sponsored enterprises, investment banks, retail banks, and electronic payment firms. Over more than a decade, the partnership has continued to grow both in terms of the size and commitment of its membership as well as the breadth of issues it addresses.

Essential to the FSSCC's success is the public sector's commitment to the public-private sector partnership outside of the already mature regulatory regime. Over the years, the FSSCC has built and maintained relationships with the U.S. Treasury and Homeland Security Departments, all the federal financial regulatory agencies (e.g., Federal Deposit Insurance Corporation, Federal Reserve Board of Governors, Office of Comptroller of the Currency, Securities and Exchange Commission), and law enforcement agencies (e.g., Federal Bureau of Investigation, U.S. Secret Service). Through these relationships, the FSSCC has directly assisted the sector's response to natural disasters, threats from terrorists, and cybersecurity events of all types. The cybersecurity threat that you highlight in your letter is one that shapes and drives many of the initiatives that we have underway with our government partners.

[1] More information regarding the FSSCC can be found at: www.fsscc.org.

Among these are:

- Enhancing information sharing, as it relates to quality and timeliness;
- Enhancing cross-sector communication and information sharing; and
- Enhancing resiliency capability and communication in response to threats.

Examples of Successful Collaborations

An example of the type of programs under these initiatives includes a project to standardize and automate the flow of cyber threat information. The resulting capability, referred to as "Soltra Edge," was implemented as a result of the direct engagement of financial sector CEOs early last year, recognizing the continually evolving threat to the sector and the need to enhance our information sharing capabilities. Leaders from our sector voluntarily came together to provide the financial support to enhance information sharing through automation and by leveraging standards that the Department of Homeland Security funded through the MITRE Corporation. Soltra Edge will greatly enhance the ability of financial services companies of all sizes (and ultimately other sectors) to assimilate and analyze threat information.

Since earlier this year, many members of the FSSCC also have been working closely with merchant/retailer associations to address cybersecurity threats affecting both of our sectors. The Merchant and Financial Cybersecurity Partnership brought together executives from the financial services and retail industries, government and other stakeholders to work together on key public policy issues to enhance information sharing between the sectors, and to deploy more robust technologies and practices. The Partnership has made progress toward its goal to work collaboratively across the payments system to enhance security in order to protect our mutual customers from cyber threats. The Partnership recently announced joint merchant and financial industry principles for information sharing legislation and is calling for Congress to act on this critical issue without delay.

Addressing Cybersecurity Risks and Attacks

Attempted cybersecurity attacks, unfortunately, are a fact of life in our increasingly cyber-connected world. Cyber-attacks range from the dissemination of malware that can infect computers and result in theft of authentication credentials to malicious Internet traffic designed to limit availability of online services thereby creating a denial of service to customers.

In most instances, financial services companies have robust security controls in place to detect malware, isolate the attempted unauthorized access, and prevent a breach from occurring. As a result, the vast majority of attempted intrusions are defeated. One analogy to compare to the physical world is a burglar casing a house, setting off an alarm while attempting to break in, and then running off to avoid the scrutiny associated with the alarm.

Given the large number of attempted intrusions, even the most secure, best run organizations can experience an intrusion that results in an actual breach. Nonetheless, financial institutions have controls in place to limit intrusions and minimize their impact, including proactively monitoring accounts, contacting customers when there are indications of suspicious activity, blocking and reissuing cards for affected accountholders, and reimbursing customers for confirmed fraudulent transactions.

The majority of reported data breaches occur outside the financial services industry. Yet, regardless of the source of the breach, when customer financial data is compromised at a third party, financial

institutions work diligently to make their customers whole, often at significant cost. When a breach does occur, it is a criminal act, victimizing the breached firm and its customers. Many of these breaches, regardless of whether they occur at a bank, a broker-dealer, a governmental agency, a retail establishment, or any other business, are perpetrated to compromise a consumer's financial information. During such events, financial services companies strive to protect their customers and cyber assets the same way they strive to protect physical assets (e.g., when bank robbers attempt to break into a bank and steal physical cash).

Over the past few years, many have interchangeably used terms like "probe", "attack", "hacked", "intrusion" and "breach" when in fact they are not synonymous. Terminology is important here. There is a difference between being attacked (happens daily to most financial firms), being breached (unauthorized access to data or funds) and losing data and/or funds (manipulation, movement, disclosure or exfiltration). A probe does not indicate an attack and an attack does not indicate a breach if it does not result in a loss of data/funds. Hence, a probe that does not result in a breach does not meet the threshold for disclosing a probe to customers. A good resource for terms: http://niccs.us-cert.gov/glossary.

The following lists a few analogies to demonstrate how typical actions by cyber criminals relate to typical actions of physical crime:

Action	***Targeting***	***Attack***	***Intrusion***	***Breach***	***Theft***	***Loss***
Meaning	Precursor actions: Looking for weaknesses identifying attack methods. One common way is via probes or scans	An attempt to gain unauthorized access to systems or data, or compromise them. Either opportunistic or targeted.	Unauthorized bypass of security mechanisms.	Unauthorized viewing, manipulation, use, movement or disclosure of sensitive data	Unauthorized taking of sensitive, protected, or confidential information or property	Quantitative measure of what was stolen directly (e.g. funds, IP) and indirectly (e.g. loss of capabilities, consumer confidence, reputation
Analogy	Like a burglar casing a house to look for an open window	Like a burglar attempting to pick a lock (targeted) or find an open window (opportunistic)	Like a burglar getting inside the house	Like a burglar finding and cracking the jewelry safe	Like a burglar taking the valuables from the safe and leaving the house	Evidence of theft/loss. Like a police report detailing what was lost/stolen

Protecting Consumers from Cybersecurity Attacks

Title V of the Gramm-Leach-Bliley Act (GLBA) requires financial regulators to develop strong requirements for financial institutions to safeguard consumer financial information. Under GLBA, the functional regulators have imposed stringent standards requiring that financial institutions maintain administrative, technical and physical safeguards to protect customer information. Since 2001, financial regulators have responded, mandating strong internal security procedures and heightened oversight of third party providers.

In addition to issuing regulations over a decade ago, the federal financial regulators have also issued "supervisory guidance" that outlines expectations and requirements for all aspects of information security and technology risk issues including authentication, business continuity planning, payments,

and vendor management (http://ithandbook.ffiec.gov/). These requirements are in addition to the myriad state laws on breach notification and data security standards.

The GLBA has thus already put in place a robust data protection and examination and enforcement system. For example, financial institutions are examined on a regular basis for compliance with the GLBA data protection requirements. Financial institutions that are found not to be in compliance are required to fix identified problems and come into compliance and are subject to various remedies, including monetary penalties and public cease and desist orders.

The GLBA and the associated regulatory requirements require financial institutions to conduct thorough assessments of the security risks to customer information and customer information systems. Moreover, if a financial institution identifies a risk, the financial institution must adopt an appropriate control to protect against the risk. A financial institution also must take steps by contract and through monitoring to oversee its service providers with access to customer information to ensure that such information is protected.

In addition, the federal banking agencies issued detailed requirements for banks, bank holding companies and their subsidiaries requiring that these entities 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.

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

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

A covered financial institution must also provide a clear and conspicuous notice. The notice must describe the incident in general terms and the type of customer information affected. It must also generally describe the institution's actions to protect the information from further unauthorized access and include a telephone number. The notice also must remind customers to remain vigilant

over the next 12 to 24 months and to promptly report incidents of suspected identity theft to the institution.

Where appropriate, the notice also must include:

- 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.

Together with these regulatory requirements, there are also strong business incentives for financial institutions to act swiftly to notify customers. Regardless of where a breach occurs, financial institutions typically bear the majority of costs including, for example, costs associated with reimbursing their customers for unauthorized transactions that occur as a result of the breach and issuing new cards/payment credentials. Swiftly notifying customers and otherwise responding to an internal or external breach impacting them not only limits a customer's inconvenience, it minimizes financial loss.

Support for Congressional Action on Information Sharing Legislation

Financial institutions have robust information security programs in place to protect their systems and customers from cyber threats. A critical resource the financial sector relies upon to safeguard their critical systems is threat information sharing, either among financial institutions, between sectors or with federal agencies. Indeed, much of the financial sector's success in preventing a successful breach of one financial institution from cascading to other companies is through swift, proactive sharing of critical cybersecurity threat information - information that describes the type of malicious code sent, the route that malware took, and the means to protect against it, particularly through the Financial Services Information Sharing and Analysis Center (FS-ISAC).

While the financial sector continues to work together and with our government partners on ways to improve the quality and timeliness of information, we have also consistently urged the Congress to further enhance cyber threat information sharing by passing legislation allowing businesses and government to better coordinate their cyber defense efforts through sharing cyber threat information, particularly across sectors.

The threat of cyber-attacks is a real and constant danger to our industry and to other critical infrastructure providers that we, and the nation as a whole, rely upon. The financial services industry is dedicated to improving our capacity to protect customers and their sensitive information. The mitigation of cyber risks to our customers, clients, partners and networks from malicious cyber activity is a critical step toward this important goal. Cyber threats are more sophisticated and dangerous than ever and require a concerted public/private partnership to identify, mitigate, and resolve, if possible. As it stands today, our laws do not do enough to foster information sharing and establish clear lines of communication with the various government agencies responsible for cybersecurity.

Along those lines, legislation is needed to strengthen the ability of the private sector and the federal government to work together to develop a more effective information sharing framework to respond to cyber threats. It should also provide narrow liability protections while strengthening, and making

explicit, privacy protections. Comprehensive cyber security legislation will enable our members to better protect their customers' personal information, thereby enhancing privacy protections.

The information the financial industry and lawmakers are talking about sharing are threat indicators that describe the type of malicious code sent toward financial institutions, the route that malware took, and the means to protect against it. This idea is very similar to law enforcement officials sharing data about physical crime with the public and media outlets when a crime occurs or is attempted. What did the perpetrator look like? What kind of weapon was used? What did the getaway vehicle look like? Where did the criminals come from? Where did they go? It is information that when shared, can be used to solve a crime or, perhaps more importantly, prevent more crime.

Conclusion

Our sector has made cybersecurity a top priority. We are committed to working with you and your colleagues in the House and Senate so that effective threat information sharing legislation can be enacted into law as soon as possible.

The financial services sector continues to support the goals of Congress to limit cybersecurity threats to business, our government, and the American people. We have appreciated the opportunity for subject matter experts from the FSSCC and the FS-ISAC to meet with House and Senate staff on numerous occasions to provide recommendations for improvement. We remain committed to this process, and would welcome the opportunity to meet with you and your staffs and work together on the important issue of improving cybersecurity across our nation in order to protect our nation's citizens.

Sincerely,

Russell Fitzgibbons
Chair, FSSCC

Doug Johnson
Vice Chair, FSSCC