Statement for the Record

by

Errol Weiss

Director of the Cyber Intelligence Center

Citi

Before the

House Financial Services Subcommittee on

Capital Markets and Government Sponsored Enterprises

Hearing on

"Cyber Security for the Capital Markets"

June 1, 2012

Good morning Chairman Garrett, Ranking Member Waters, and members of the Subcommittee:

My name is Errol Weiss; and I am the Director of Citi's Cyber Intelligence Center, which is responsible for collecting, analyzing, and exchanging threat intelligence in an effort to protect the Citi brand, global business operations, technology infrastructure and client trust against cyber threats world-wide. This morning I am testifying on behalf of the Securities Industry and Financial Markets Association (SIFMA) on how to best protect capital markets from emerging cyber threats.[1]

I. Introduction

SIFMA supports the goals of the Administration and Congress to limit cybersecurity threats to the American people, businesses, and government through a more integrated approach. The increase in cyber intrusions and cyber crimes in the past decade is cause for great concern, particularly to those in the financial services sector. SIFMA member firms are on the front lines defending against cyber threats to the financial markets and we take this role very seriously.

[1] The Securities Industry and Financial Markets Association (SIFMA) brings together the shared interests of hundreds of securities firms, banks and asset managers. SIFMA's mission is to support a strong financial industry, investor opportunity, capital formation, job creation and economic growth, while building trust and confidence in the financial markets. 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.

At the outset, we think it's important for Members of Congress and the Administration to understand the existing regulatory framework under which the financial services industry functions.

II. The Existing Cybersecurity Infrastructure of the Financial Services Sector

The United States has embraced a sector-specific approach to data security and privacy regulation for decades. SIFMA urges Congress to consider the unique position of the U.S. financial services sector in connection with the ongoing examination of the national cybersecurity framework. As part of the financial services industry, SIFMA members are currently subject to stringent laws and regulations on the protection of personal data, including the Gramm-Leach-Bliley Act (GLBA), the Fair Credit Reporting Act (FCRA) and the Right to Financial Privacy Act (RFPA). These laws and regulations are reinforced by regular, pro-active review, and audited by highly specialized regulators that are supported by the Federal Financial Institutions Examination Council (FFIEC), an interagency entity that issues data privacy and cyber security guidance and monitoring procedures. As discussed below, financial services firms appreciate more than almost any other sector of the economy the importance of maintaining the confidentiality of customer information. The financial services industry is keenly aware of the consequences resulting from a privacy or security lapse, and has long played a leadership role in developing policies, procedures, and technology to protect customer data.

The financial services sector has had an effective and longstanding working relationship with the U.S. Treasury Department on cybersecurity since Presidential Decision Directive/NSC-63 was issued in May 1998. In response, the industry proactively formed the Financial Services Information Sharing and Analysis Center (FS-ISAC)[2] which began operations in October 1999. After September 11, 2001, and in response to Homeland Security Presidential Directive 7 (HSPD7) and the Homeland Security Act, the FS-ISAC expanded its role to encompass physical threats to our sector that could impact business continuity and resiliency. Citi was one of the founding members of the FS-ISAC and I am currently on the FS-ISAC Board of Directors. A key factor in the success of the FS-ISAC is trust. And trust takes years to develop. The FS-ISAC has worked hard to facilitate the development of trust between its members, with other organizations in the financial services sector, with other sectors, and with government organizations such as law enforcement, regulators, and intelligence agencies for over a decade. We cannot afford to weaken that trust.

In addition to the work and success of the FS-ISAC the financial services industry is already one of if not the most highly regulated industries from a cybersecurity standpoint. SIFMA members are currently subject to the FCRA, GLBA and the examination guidelines of the FFEIC. Since 1970, the FCRA has promoted the accuracy, fairness, and privacy of personal data assembled by "consumer reporting agencies" (CRAs), including data provided by a majority of SIFMA member firms. The FCRA establishes a framework of fair information practices that include rights of data quality, data security, identity theft prevention, and use limitations, requirements for data destruction, notice, user consent, and accountability.

[2] For an overview of the FS-ISAC's responsibilities and functions, please visit: http://www.fsisac.com/files/FS-ISAC_Overview_2011_05_09.pdf

The GLBA provides data privacy rules applicable to "financial institutions," a term defined broadly to cover entities significantly engaged in financial activities such as banking, insurance, securities activities, and investment activities. The GLBA imposes data privacy obligations such as the obligation to securely store personal financial information, and provide data subjects with notice of the institution's privacy practices and the right to opt-out of some sharing of personal financial information. The GLBA regulations also provide guidelines to financial institutions on appropriate actions in response to a breach of security of sensitive data, including on investigation, containment, and remediation of the incident and notification of consumers and/or law enforcement authorities when warranted.

Finally, many SIFMA member firms also follow FFIEC guidance and monitoring procedures. The FFIEC is an interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Office of Thrift Supervision.

The FFIEC also makes recommendations to promote uniformity in the supervision of financial institutions. In the area of cybersecurity and data breach protection, the FFIEC has published the following standards: FFIEC Interagency Guidelines Establishing Standards for Safeguarding Customer Information; FFIEC Interagency Guidelines Establishing Information Security Standards; FFIEC Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice; FFIEC Information Technology Examination Handbook (includes guidance and audit provisions of many of the requirements identified in the guidance documents referenced above).

III. Proactive Sector Initiatives

FS-ISAC Account Takeover Task Force

In 2010, the FS-ISAC formed the Account Takeover Task Force (ATOTF) as a result of continued concern and need for additional tools to help financial institutions and their customers combat online account takeover attacks. The ATOTF consists of over 120 individuals from thirty-five financial services firms of all sizes and types, ten industry associations and processors and representatives from seven government agencies. The ATOTF focuses on deliverables in three areas of effective cyber defense: Prevention, Detection and Response.

Some example deliverables and products produced by the ATOTF include:

Prevention

- Fraud Advisory for Businesses: Corporate Account Take Over, co-branded with US Secret Service, FBI and Internet Crime Complaint Center (IC3). The advisory is available here: http://www.fsisac.com/files/public/db/p265.pdf

- Fraud Advisory for Consumers: Involvement in Criminal Activity through Work from Home Scams, co-branded with FBI and IC3. The advisory is available here: http://www.fsisac.com/files/public/db/p264.pdf
- J1-Visa Money Mule Advisory
- Internet Auto Fraud

Detection

- Detection Whitepaper for financial institutions – Document focused on detection of account takeover victims.
- Techniques for recovering customers from ZeuS or other keystroke logging/man-in-the-middle Trojan infections and the exploration of third-party services with the goal of gathering elements of intelligence to enable better detection methods.
- Document Standard Set of Requirements and enhancements for alerting and security requirements for core ACH/wire transfer software providers.

Response

- Contact List, Procedures - This list provides financial institutions the information they need to report account takeover attacks via online banking to the Secret Service, FBI and other agencies, and a process for keeping the contact lists current.
- Form for Reporting account takeovers, including what should be submitted in the incident report and used for metrics to measure the success of the ATOTF.
- Actions financial institutions can take after an incident, communicated via FS-ISAC advisory notices.
- Internet Fraud Alert service from the National Cyber-Forensics & Training Alliance (NCFTA). This provides financial institutions with information for recovered credentials from the takedown of botnet command and control servers.
- List of Resources currently available for cyber crime and broad education so that financial institutions can leverage existing resources.
- Malware Submission method provides a process for sharing identified new malware with government/law enforcement agencies and anti-virus vendors.
- Redesign Suspicious Activity Report (SAR) Submission and Analysis Process by working with the Financial Crimes Enforcement Network (FinCEN) to give financial institutions and regulators more actionable information.
- Recommendations for reporting an account take over attack via SARs.

Finally, the ATOTF implemented a survey and polled member organizations regarding commercial account takeover to establish a baseline for Commercial Account Takeover attempts and losses. The surveys collected data in 2009, 2010 and the first half of 2011. The results indicate that financial institutions are doing a better job of stopping fraudulent transactions.

Botnet Takedown Partnership with Microsoft

FS-ISAC, in partnership with Microsoft and NACHA, announced on March 26, 2012, that they successfully executed a coordinated global takedown operation against some of the most

notorious cybercrime operations responsible for online fraud and identity theft. The takedown was accomplished through coordinated legal and technical actions and disrupted massive botnets using the ZeuS and SpyEye malware families, striking a major blow against cybercriminal operators targeting the financial services sector's customers.

A video news release about the disruption, codenamed, "Operation B71", is located here at the Microsoft Digital Crimes Unit web page: http://www.microsoft.com/presspass/presskits/dcu/ . The takedown will help prevent online fraud and identity theft for consumers and businesses worldwide. Microsoft's investigation shows that approximately 3.6 million computers in the United States alone have been infected with the ZeuS malware.

This takedown was made possible through a successful pleading before the U.S. District Court for the Eastern District of New York on March 19, 2012, which allowed Microsoft, FS-ISAC and NACHA to sever the command and control structures of several of the most dangerous botnets running ZeuS, SpyEye and Ice IX malware. Because the botnet operators used ZeuS, SpyEye and Ice IX to steal victims' online banking credentials and transfer stolen funds, FS-ISAC and NACHA joined Microsoft as plaintiffs in the civil suit.

On March 23, 2012, Microsoft and co-plaintiffs FS-ISAC and NACHA, escorted by the U.S. Marshals Service, executed a coordinated physical seizure of servers in multiple hosting locations to preserve evidence for this case and seized hundreds of domain names used by the ZeuS, SpyEye and Ice IX malware to remotely command and control victim computers. Although it is not expected that this operation will completely destroy all botnets running ZeuS, SpyEye and Ice IX malware, or even that every botnet taken down in the operation will stay down permanently, this action is expected to significantly disrupt the cybercriminals' operations by increasing the risk and costs for its controllers to continue doing business.

Microsoft has stated that it will use the intelligence gained from this takedown to partner with Internet Service Providers and Computer Emergency Response Teams around the world to help remediate infected computers from the control of ZeuS, SpyEye and Ice IX, making the Internet safer for consumers and businesses worldwide.

Together, these aspects of the operation are expected to undermine the criminal infrastructure that relies on these botnets every day to make money and helps to provide new tools for the industry to work together to proactively fight cybercrime.

IV. The Threat - Hactivists, Organized Crime and Nation States.

Threats to the banking and finance sector come primarily from three groups – hacktivsts (on-line activists promoting a sociopolitical ideology), organized criminal gangs (committing cybercrime for financial gain), and foreign nation states / extremist groups (committing industrial espionage to gain competitive advantage or disrupt financial markets).

Hacktivism is a term used to describe motivated individuals and groups that use hacking techniques to promote a political ideology. While traditionally cyber based, in 2011, we witnessed hacktivist causes spill over into the physical world as well, causing disruptions and

complicating business operations for many government and businesses, including SIFMA members. Starting as far back as 1994, hacktivists were using Distributed Denial of Service (DDoS) attacks to make internet sites and services unavailable to intended users. DDoS attacks have since become a staple hacktivist technique, resulting in lost revenue and reputational damage. In the past year, hacktivist activity has exploded, with malicious actors bent on retaliation against organizations that do not support their cause. Hacktivist tactics continue to include DDoS attacks and also include public exposure of sensitive internal information.

Sophisticated criminal organizations continue to target individuals and organizations with sensitive financial information. Once they are able to compromise a victim, criminals are quickly turning the stolen data into financial gain. The criminals operate a sophisticated and mature business, with a complete operating model that includes outsourcing of each discrete component of the underground ecosystem to specialists and experts around the globe. Criminals cooperate through the development of malware to evade anti-virus protections, the delivery of malware via targeting phishing emails and/or infected websites, stealing customer credentials and answers to challenge questions, takeover of on-line banking accounts, and movement of stolen money through a network of unwitting and/or complicit professional "money-mules" to the criminal syndicate often outside the U.S. in places like Eastern Europe.

Technically advanced and adversarial Nation States and extremist groups represent the third major threat to the banking and finance sector. Foreign economic collection and industrial espionage against the United States and other nations are conducted, to a large degree, in Cyberspace. Virtually every business activity and the creation of new ideas take place on the Internet. Malicious actors, whether they are corrupted insiders or foreign intelligence operatives, can easily steal and transfer massive quantities of data while remaining anonymous and nearly impossible to detect. Foreign operatives with motivation to steal sensitive economic information are able to operate in cyberspace with relatively little risk of getting caught.

The use of sophisticated malware, along with highly cooperative hackers for hire, makes it difficult to attribute responsibility for the entities behind corporate computer network intrusions. Foreign adversaries perform industrial espionage to target proprietary (and sometimes non-proprietary) company information they can use for their own gain. For a SIFMA member firm, foreign adversaries could be interested in information like client lists, merger and acquisition data, company information on pricing, and financial data. High technology firms may be targeted for new design information. Extremist groups use the same techniques to gain system access, but go a step further by using that access to cause disruption and/or destruction. As an example, recent DDoS activity against large U.S. member firms has been orchestrated by extremist and terrorist groups associated with foreign nation states.

V. Information Sharing

Despite the robust cybersecurity infrastructure that the financial services sector has established and the current ability to share information with our peers and others, SIFMA recognizes the need for expanded information sharing with government agencies, including greater private sector access to threat data from Federal intelligence and law enforcement agencies. Access to threat information must be administered in a manner that can provide broader cybersecurity

protection without compromising ongoing investigations or the privacy of individual Americans. In addition, providing greater access to security clearances for private sector employees will increase the likelihood that cyber threat information will be distributed in a timely manner and handled properly.

While we support enhanced transparency and information sharing, we are concerned that if sensitive private sector information is shared with a government agency, it could be divulged to the public in response to a Freedom of Information Act (FOIA) request. Such disclosure could invite further attacks or create the perception that an institution is defending itself ineffectively. SIFMA believes that cybersecurity information shared with government agencies, including the identification of critical infrastructure, must be exempted from disclosure under FOIA.

Additionally, SIFMA believes government agencies should leverage ISACs and the United States Computer Emergency Readiness Team (US-CERT) to facilitate two-way and cross-sector public/private information sharing. We believe the ISACs should remain in place for mature sectors like financial services and we oppose any cybersecurity legislation that establishes a "National Information Sharing" clearinghouse, which will add layers of bureaucracy and delay information sharing with existing ISACs.

VI. Recent Cybersecurity Proposals

This past fall, the House Cybersecurity Task Force recognized that private-sector entities control the vast majority of U.S. information and communications technology and other critical infrastructure. These entities are in the best position to identify and defend against cyber-related threats. Owners and operators are, and should be, responsible for the protection, response, and recovery of private assets. Yet, there is widespread agreement that the public and private sectors need to work together, particularly when it comes to greater sharing of information in order to achieve enhanced situational awareness to detect, prevent, mitigate, and respond to emerging and rapidly changing threats – while at the same time ensuring that personal information is adequately protected.

In the spirit of enhancing public-private coordination, several members of Congress drafted proposals to combat cyber threats to critical infrastructure; increase public/private information sharing regimes; increase cyber research, development and education; and update federal network security practices.

SIFMA is especially encouraged by the information sharing provisions contained within CISPA, introduced by Reps. Mike Rogers (R-MI) and Dutch Ruppersberger (D-MD)

SIFMA believes the sharing of information from government to industry has immense value but we are also supportive of the voluntary approach to information sharing from the private sector to the government. CISPA provides a solid framework and useful legal protections to encourage and permit the timely flow of actionable information. Creating an environment where cyber threat intelligence is readily available and shared is fundamental to any long-term endeavor to defend our country and make our markets more resilient.

As the debate continues in Congress, in addition to information sharing, SIFMA asks that Members keep the following principles in mind with respect to the following issues:

1. **Critical Infrastructure:** Several of the recent cybersecurity proposals include provisions that grant DHS the ability to designate an organization as a critical infrastructure operator and then regulate that system or organization. SIFMA believes that the financial services sector's current regulator is best-suited for the role of designating or regulating a critical infrastructure operator because they have a long history and are familiar with the complex operations of financial services organizations. The Treasury Department, as the Sector Specific Agency for the financial services sector, and the regulatory agencies through the Financial and Banking Information Infrastructure Committee (FBIIC), should determine if an institution in the sector is considered critical. The financial industry, like many other industries in the United States, is far too complex to be managed and regulated via a one-size fits all solution.

   Furthermore, when determining what constitutes critical infrastructure within a firm, the scope of critical infrastructure should apply to specific capabilities, processes, functions or business units and not to an entire firm or institution. It must be recognized that critical infrastructure is built within an ecosystem that includes commercial vendors and suppliers that contribute to the overall resiliency of the capability, process or function that should be protected. SIFMA supports enhanced supervision over service providers on which financial institutions depend (e.g., hardware and software providers, Internet service providers, etc.); however, such coordination may be better achieved by building on some of the existing mechanisms that seek to address these issues (e.g., Partnership for Critical Infrastructure Security).

   Building on existing mechanisms and organizations within the sector, we feel it is essential that the private sector have a prominent voice in the criteria that will be used to designate critical infrastructure. By leveraging the established partnership between the Financial Services Sector Coordinating Council (FSSCC) and the FBIIC, the experts can come together and determine what the criteria, metrics and thresholds should be to determine if a specific capability, process, function or business unit within the financial services industry is critical. Once those systems are denoted, leveraging and updating the existing rules in place that we as an industry already adhere to would make implementation and assessment as seamless as possible.

2. **Supply Chain:** SIFMA supports federal cybersecurity supply chain management and promotion of cybersecurity as a priority in Federal procurement. Other efforts to defend against cybersecurity threats will be lessened without financial support for the infrastructure necessary to implement a defense strategy.

3. **Law Enforcement:** SIFMA supports the strengthening and clarification of criminal penalties for cybercrimes. These improvements further bolstered by an increase in budgets and personnel for these purposes at law enforcement agencies will provide additional protection for consumers and financial institutions.

4. **Research & Development:** The development of essential technologies and improving federal systems are important efforts which should be supported. As DHS and the National Institute of Standards and Technology (NIST) pursue their research and development agendas, we hope to see substantial resource commitments and advances in these areas. We also support the improvement of the resilience and security of federal systems to further prevent cybercrime.

5. **International Cooperation:** Because cybersecurity is a global problem and cyber crimes frequently occur across borders, cooperation with international partners is critical to preventing, investigating, and prosecuting cyber crime. The U.S. should seek strong cooperation with foreign governments, international law enforcement agencies and policy making bodies, to improve cybersecurity. The U.S. should pressure foreign governments to enact effective cyber security legislation and demonstrate they enforce those laws by prosecuting and punishing individuals convicted of such crimes. If we do not work across borders on this issue our ability to prevent, defend and deter cyber crimes will be severely limited.

6. **Safe Harbor for Disclosure:** SIFMA members believe that the safe harbor provisions for cybersecurity reporting will be helpful for SIFMA members and provide much-needed extra protections for sharing information beyond what is currently available under Protected Critical Infrastructure Information (PCII) provisions. Financial institutions that cooperate with the government in cyber-threat sharing should receive liability and confidentiality protections. We are in support of both strong liability and confidentially protections with strong preemption.

7. **Education & Awareness:** Public education and awareness campaigns have been a critical method of limiting cyber crimes in the financial services industry. Both the Securities and Exchange Commission (SEC) and SIFMA members have promoted public awareness of the risk of disclosure of personal information for many years, and SIFMA supports the expansion of any such campaigns and promotions.

8. **Breach Notification:** SIFMA members believe that a single, uniform federal breach notification standard that preempts state law would help reduce administrative oversight, establish clear notification guidelines, and reduce consumer confusion. We support a notification standard that is based on risk-based assessments of actual or likelihood of harm, and allows for a reasonable investigation and mitigation period.

VII. Conclusion

SIFMA supports the efforts of the Administration and Congress to further protect the American people, businesses, and government from the increasing threat of cyber attacks and cyber crimes. As you can see, the financial services sector faces a number of significant threats and is currently tracking several of them, with a concern that they may materialize in the future. We have outlined a number of the actions that the FS-ISAC has taken on behalf of the sector to identify and mitigate threats that we are facing. In addition, the financial services sector already has a strong regulatory regime in place with its existing regulators. This oversight, as well as

partnerships with industry bodies and software providers, allows us to proactively work to ensure that our systems are protected and that we maintain flexibility so that we can respond quickly when threats change.

Recent proposals are a good first step in addressing some of the issues and the four bills recently passed by the House address many of the principles we laid out earlier. The changes to the Federal Information Security Management Act (FISMA) that will drive improvements in federal systems, increase coordination between federal agencies around education, awareness, standards and talent development, and the reauthorization of the Networking and Information Technology Research and Development program (NITRD), will assist in helping America better protect its cyberspace. CISPA in particular will move us along the furthest by making the private sector aware of the threats that are out there and provide a framework within which we can confidently share information with the government.

The sharing of actionable and timely intelligence will allow the people with the greatest expertise in protecting their systems, many of them critical to properly functioning markets and the economy at large, the best chance of anticipating, protecting and defending their systems and networks from the individual criminals, criminal syndicates and nation states that seek to steal intellectual property, disrupt markets and do harm.

SIFMA members are accustomed to and fully supportive of protecting their customers' data, and, as partners and service providers, the data of customers of financial institutions worldwide. Encouraging effective data protection goes to the heart of SIFMA's mission of building trust and confidence in the financial services industry. Without effective protection of the personal data of our customers, financial institutions would lack the public trust that is so critical for their operation.