

STATEMENT
OF
SECURITIES INDUSTRY AND FINANCIAL MARKETS ASSOCIATION
("SIFMA")
BEFORE THE
UNITED STATES HOUSE OF REPRESENTATIVES HOMELAND SECURITY
SUBCOMMITTEE ON CYBERSECURITY, INFRASTRUCTURE PROTECTION AND
SECURITY TECHNOLOGIES
EXAMINING THE HOMELAND SECURITY IMPACT OF THE OBAMA
ADMINISTRATION'S CYBERSECURITY PROPOSAL
JUNE 24, 2011

I. Introduction

SIFMA supports the goals of President Obama and Congress to limit cybersecurity threats to the American people, businesses, and government through a more integrated approach to fighting these threats. The increase in cyber intrusions and cyber crimes in the past decade is cause for great concern, particularly those in the financial services sector. SIFMA member firms are on the front lines of defense against cyber threats to the financial markets and we take this role very seriously. On May 12, 2011, President Obama released an extensive proposal (“Proposal”) which is intended to bolster the American cybersecurity infrastructure and protect Americans from cyber threats. Although SIFMA supports the ultimate goals of the Proposal, we are concerned that the Proposal does not adequately take into consideration the extensive existing regulatory framework under which the financial services industry functions.

SIFMA brings together the shared interests of more than six hundred securities firms, banks, and asset managers throughout the world. By building trust and confidence in the financial industry SIFMA intends to encourage capital availability, job creation, and economic growth. 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 their customers, financial institutions would lack the public trust that is so critical for their operation.

SIFMA's members include some of the largest financial institutions in the world. As part of the financial services industry, SIFMA members are currently subject to stringent laws and regulation 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. These laws and regulations are reinforced by regular, pro-active review and audit by highly specialized regulators. Consequently, 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.

II. Importance of recognizing uniqueness of the financial services sector

The United States has for decades embraced a sector-specific approach to data security and privacy regulation. As a result, health and financial information are subject to extensive regulation that was crafted for the unique circumstances presented by those industries. Applying general data security

and privacy concepts to those industries is not only unnecessary, it could be inconsistent with existing regulations and produce unintended negative consequences.

SIFMA urges Congress to consider the unique position of the U.S. financial services sector in connection with the ongoing examination of national privacy framework. As discussed below, financial services firms appreciate more than almost any sector of the economy the importance of maintaining the confidentiality of customer information. The financial services industry is keenly aware of the potential for tangible harm that could flow 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 industry has had an effective and longstanding engagement 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”). The industry has committed significant time and effort to integration with the Department of Homeland Security (“DHS”) through US-CERT and the National Cybersecurity and Communications Integration Center (“NCCIC”). In addition, the FS-ISAC is already in the process of embedding appropriately cleared staff in the NCCIC.

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, use limitations, requirements for data destruction, notice, user consent, and accountability.

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 and the regulations issued under the GLBA help to protect valuable customer information and to prevent data breaches. Through exceptionally broad definitions,

GLBA protections apply to virtually all personal information about individual consumers or customers held by more than 40,000 financial institutions in the United States - including less traditional “financial institutions” such as check-cashers, information aggregators, and financial software providers. Moreover, the GLBA and its implementing regulations require financial institutions not only to limit the disclosure of customer information, but also to protect that information from unauthorized accesses or uses. 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.

Many SIFMA member firms also follow the Federal Financial Institutions Examination Council (“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).

Finally, many SIFMA member firms who process government loan data must comply with the Federal Information Security Management Act of 2002 (“FISMA”) and the Federal Information System Controls Audit Manual 2009 (“FISCAM”). FISMA emphasizes the need to develop, document, and implement an enterprise-wide program to provide information security for the information and information systems that support the operations and assets of the Federal government, including those provided or managed by another agency, contractor, or other source. FISMA directs the promulgation of federal standards for: (i) the security categorization of federal information and information systems based on the objectives of providing appropriate levels of

information security according to a range of risk levels; and (ii) minimum security requirements for information and information systems in each such category.

In accordance with FISMA, the National Institute of Standards and Technology (“NIST”) develops the guidance and procedures which directly pertain to security control implementation, continuous monitoring, independent assessment, and risk analysis. The NIST Federal Information Processing Standard (“FIPS”) Publication 200, “Minimum Security Requirements for Federal Information and Information Systems,” specifies minimum security requirements for federal information in seventeen security-related areas. These minimum security requirements are defined through the use of the security controls provided by NIST Special Publication 800-53 rev3, “Recommended Security Controls for Federal Information Systems.”

FISCAM is designed to be used primarily on financial and performance audits and attestation engagements performed in accordance with generally accepted government auditing standards (“GAGAS”), as presented in Government Auditing Standards (also known as the "Yellow Book"). FISCAM is also consistent with the GAO/PCIE Financial Audit Manual (“FAM”). Additionally, FISCAM control activities are consistent with NIST Special Publication 800-53 rev3 controls.

III. Support for the Proposal

A. Improved Coordination Across Agencies and Sectors

SIFMA believes the Proposal takes many important steps to ensuring a safer cyber community and SIFMA fully supports those efforts. The Federal government should be leading the proactive defense against cybersecurity threats and take coordinated action to protect critical infrastructure from such attacks. SIFMA members rely heavily on other sectors such as telecommunications, information technology, energy, and transportation which are frequently at risk for cyber attacks. SIFMA supports enhanced supervision over service providers on which financial institutions depend (*e.g.*, hardware and software providers, Internet service providers, etc.). Such coordination may be achieved by building on the existing mechanisms that seek to address these issues (*e.g.*, Partnership for Critical Infrastructure Security).

Moreover, SIFMA believes that cyber threats can be best fought through a coordinated defense network across agencies and business sectors. Such an infrastructure would improve communication and enforcement mechanisms. Coordination should occur at the agency level where agencies can report cyber threats through pre-determined channels whereby threats can be reviewed and analyzed consistently, regardless of source. Individual firms should not be required to report cyber attacks and threats to multiple agencies under multiple reporting regimes. Such a structure is inefficient and may delay defensive measures.

SIFMA also supports the Administration's commitment to two-way public/private information-sharing, leveraging the Information Sharing and Analysis Centers (ISACs), the US-CERT, safe harbors, clearances, and confidentiality guarantees. As an example, the Financial Services - Information Sharing and Analysis Center (FS-ISAC) constantly gathers reliable and timely information from financial services providers, commercial security firms, federal, state and local government agencies, law enforcement and other trusted resources. FS-ISAC is uniquely positioned to quickly disseminate physical and cyber threat alerts and other critical information to participating organizations, including analysis and recommended solutions from leading security industry experts. SIFMA also believes there is opportunity to accelerate information flow on a cyber event without compromising sensitive information. This can be done through segmentation, protocols, and decision trees.

SIFMA also 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.

B. Law Enforcement

SIFMA supports the strengthening and clarification of criminal penalties for certain cybercrimes. Such expansion will provide additional protection for consumers and financial institutions from financial crimes. These improvements are further bolstered by the increase in budgets and personnel for these purposes at law enforcement agencies.

C. Technology and International Cooperation

SIFMA believes that the development of essential technologies and improving federal systems are important efforts which should be supported. As DHS and NIST pursue their research and development agendas, and as the Administration pursues its recently announced International Strategy for Cyberspace, we hope to see substantial resource commitments and advances in these areas. SIFMA also supports the improvement of the resilience and security of federal systems to further prevent cybercrime.

D. Cooperation with International Partners

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. Without strong cooperation with international law enforcement agencies, U.S. efforts to improve cybersecurity will be severely limited.

E. Safe Harbor for Voluntary Disclosure

SIFMA members believe that the safe harbor provisions for cybersecurity reporting under Sec. 245, “Voluntary Disclosure of Cybersecurity Information,” 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.

F. Safe Harbor for Encrypted Information

Although SIFMA has reservations about several aspects of the data breach notification provisions, SIFMA is supportive of the safe harbor in Section 102(b) whereby if the data which is the subject of a breach is “unusable, unreadable, or indecipherable through a security technology” there is a presumption of no reasonable risk. Currently, not all states allow for such a presumption, so a consistent federal standard for such a presumption would be helpful when assessing a security breach. Our other concerns related to the data breach notification provisions, are set forth in the next section below.

G. Public Education and Awareness

Public education and awareness campaigns have been a critical method of limiting cyber crimes in the financial services industry. Both the 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.

IV. SIFMA Concerns with the Proposal

A. Data Breach Notification

SIFMA members are concerned that the data breach notification provisions in the Proposal are unduly burdensome as currently drafted. Although SIFMA believes a preemptive data breach notification standard would serve the industry well, the Federal Trade Commission (“FTC”) reporting requirements in the Proposal are potentially more burdensome than the existing web of state data breach notifications laws and regulations. SIFMA believes that a reasonable federal data breach notification standard would help reduce cybercrime and protect individuals and businesses from unnecessary losses. To reach that standard, however, SIFMA believes the Proposal should be changed to incorporate several critical concepts as outlined below.

1. Definition of Security Breach

As proposed, the definition of “Security Breach” is significantly broader than most existing state data breach notification requirements. SIFMA recommends a definition similar to several state laws that would define security breach as “unlawful and unauthorized acquisition of computerized data that materially compromises the security, confidentiality, or integrity of personal information maintained by the person.” See, e.g., Fla. Stat. § 817.5681(4). SIFMA also asserts that there should be a good faith exception for employees or agents of the firm for businesses purposes so long as there is no further unauthorized disclosure or use of such information. See, e.g., N.Y. GBS. LAW § 899-aa.

2. Definition of Sensitive Personally Identifiable Information

SIFMA believes that the current definition of “Sensitive Personally Identifiable Information” is unduly broad and if left unchecked would increase compliance costs severely without preventing data breach. Leaving the definition open to FTC interpretation and rulemaking creates additional uncertainty. The definition in the Proposal includes a social security number or driver’s license number without any other information. Existing state laws generally define “personal information” as a person’s name or other identifying information *in conjunction with* a social security or driver’s license number. See, e.g., Fla. Stat. § 817.5681(5). The disclosure of a social security or driver’s

license number without any other identifying information should not trigger data breach notification requirements because such information has limited or no value. Requiring firms to undergo a risk assessment and FTC report every time such a piece of information is misdirected in good faith would require multiple reports per week.

In addition, the definition in Section 1(g)(4) of the Proposal also includes “a unique account identifier, including a financial account number or credit or debit card number, electronic identification number, user name, or routing code.” Yet, Section 1(g)(5) requires such information in (g)(4) *plus* a name or security code to trigger the notification requirements. SIFMA proposes deleting paragraph (g)(4) as duplicative and unnecessarily broad. If section (g)(4) is passed as written, the daily business ramifications for SIFMA member firms would be extensive. Among others, account numbers are necessary for financial firms to transact its business as well as for allocation to ensure that transactions are aligned with proper account information. If transaction information is misdelivered and happens to contain only account numbers, the firm would have to conduct a risk assessment and report the results to the FTC. Those efforts would far outweigh any benefit reaped from such an innocuous disclosure.

3. FTC Reporting Requirements (Safe Harbor Exemption)

The Proposal’s exemption under Sec. 102(b) provides a safe harbor from enforcement when a firm determines that there is no risk of harm to an individual from a security breach. The qualifying firm will not send a notice to that individual if within 45 days the firm submits to the FTC a written risk assessment justifying the conclusion of no harm. SIFMA believes that performing a risk assessment and submitting such results to the FTC for every Security Breach no matter how small or insignificant mitigates the potential benefit of having such a safe harbor. As currently drafted, even a small data misdirection between financial institutions due to an error would constitute a Security Breach and thus would require the firm to perform a risk assessment and submit the results to the FTC. This result is in spite of the fact that the “unauthorized party” is in fact another financial institution covered by the same legal, regulatory and operational controls and there with only minimal risk for harm to the customer. Consequently SIFMA believes that this provision is not actually a safe harbor, but rather an additional layer of reporting obligation. We would recommend that this provision be amended to only cover material Security Breaches, such that a small or

insignificant misdirection of data, particularly when the recipient is a regulated entity, should not trigger these requirements.

4. Effective Date

SIFMA members are concerned that the effective date of 90 days after enactment for the data breach notification requirement is too short. The timeframe does not give the FTC adequate time to propose and adopt clarifying regulations. In addition, firms must make corresponding changes to policies and procedures, as well as modify their reporting systems. The new notification and disclosure provisions will require training and hiring of new staff, which will be difficult to achieve in a 90 day period.

B. Covered Critical Infrastructure

1. DHS as a Cybersecurity Regulator

As currently drafted, the Proposal centralizes domestic cybersecurity responsibilities in DHS, thus making DHS a regulator as well as an enforcer. The addition of DHS into the web of financial services regulation may cause complications for both regulators and regulated financial services firms. SIFMA would prefer for the existing financial regulators to continue as primary regulators for the firms. The financial regulators could then coordinate with DHS and the FTC to the extent necessary, but the firms would not be required to report directly to DHS.

DHS is primarily a technical coordination agency for cybersecurity but DHS has no fundamental understanding of the many business functions performed by the financial services sector. Sector Specific Agencies (“SSAs”), such as the Department of Treasury, under Homeland Security Presidential Decision Directive 7 and the National Infrastructure Protection Plan, play a significant role for the sector in providing business understanding and advocacy.

In addition, there is a technical capability gap between DHS, the NSA, and U.S. Cyber Command (“CYBERCOM”). NSA, CYBERCOM, and all intelligence community members need to be subordinate technical and operational resources that DHS coordinates to support critical infrastructure. These agencies need to be subject to the mandate of the National Infrastructure Protection Plan (“NIPP”) and function to coordinate all engagement with CI/KR sectors through DHS and the SSAs. DHS would be responsible for the incident response process and national

technical coordination. For the financial services industry, the Department of Treasury, along with the SEC, CFTC, Federal Reserve Board and others, would handle mission, business, and regulatory coordination.

2. Identifying Critical Infrastructure Operators

The Proposal gives DHS the authority to designate an organization as a critical infrastructure operator. SIFMA believes that DHS is not well-suited to this role because of its lack of familiarity with the operations of financial services organizations. The Treasury Department, as the Sector Specific Agency for the financial services sector, and the regulatory agencies through the FBIIC, should determine if an institution in the sector is considered critical, not DHS.

3. Risk Mitigation Framework & Evaluation

The Proposal would require critical operators to develop a framework to address cyber threats, and engage a third-party commercial auditor to assess such plans. These requirements would impose significant additional administrative burdens on financial services firms which are already subject to intense regulation. Although engaging an independent auditor significantly increases defense against cyber threats, it does not guarantee effectiveness. It also appears that DHS and NIST would have the ability to modify a firm's framework, which raises many questions for SIFMA members.

4. Public Disclosure of Cybersecurity Plans

SIFMA is also concerned about the requirements in the Proposal under Section 7(b) which would require the critical infrastructure operators to publicly disclose high-level summaries of their cybersecurity plans and whether those plans are working effectively. SIFMA believes that any disclosure of cyber defensive mechanisms may give criminals information which may help them to carry out a cyber crime.

V. Conclusion

SIFMA supports the efforts of President Obama and Congress to further protect the American people, businesses, and government from the increasing threat of cyber attacks and cyber crimes. SIFMA believes that this Proposal could help achieve those goals if the amendments suggested in this statement are implemented. Without such changes, this Proposal will have diminished value and could do more harm than good for SIFMA members and their customers.