sifma

Invested in America

January 31, 2011

Via Electronic Mail (privacynoi2010@ntia.doc.gov)
National Telecommunications and Information Administration
U.S. Department of Commerce
1401 Constitution Ave., NW, Room 4725
Washington DC 20230

Via Electronic Submission
(https://ftcpublic.commentworks.com/ftc/consumerprivacyreport**)**
Federal Trade Commission
Office of the Secretary, Room H-113
600 Pennsylvania Avenue, NW
Washington, DC 20580

Re: Department of Commerce Report: *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework*
Federal Trade Commission Report: *Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers*

Dear Sir or Madam:

The Securities Industry and Financial Markets Association ("SIFMA")[1] appreciates the opportunity to comment on the Department of Commerce ("DOC") report *Commercial Data Privacy and Innovation in the Internet Economy: A Dynamic Policy Framework* and the Federal Trade Commission ("FTC") report "Protecting Consumer Privacy in an Era of Rapid Change: A Proposed Framework for Business and Policymakers."

The following discussion provides some background on the extensive privacy and data security regulations that currently exist for the financial services industry. A number of the proposals in the DOC and FTC reports are then discussed. Because existing laws and regulations provide strong data privacy protections for financial services customers, and because the securities industry has a rigorous self-regulatory structure in place that has worked well for decades, SIFMA recommends that industries already subject to sectoral regulation, such as financial

[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 develop policies and practices which strengthen financial markets and which encourage capital availability, job creation and economic growth while building trust and confidence in the financial industry. SIFMA, with offices in New York and Washington, D.C., is the U.S. regional member of the Global Financial Markets Association (GFMA).

services, be excluded from both agencies' final reports which are understandably principally focused on sectors of the economy that are not currently subject to privacy regulations. As to those other sectors, SIFMA recommends that the example of financial services privacy regulation be kept in mind, both because the process of developing such regulation took into account the unique aspects of financial products and services, and because the resulting regulations strike the right balance between consumer and industry interests.

I. Privacy Policy Goals for the Financial Services Industry

SIFMA urges the FTC and DOC 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. Financial services are keenly aware of the potential for tangible harm that could flow from a privacy or security lapse, and have long played a leadership role in developing policies, procedures, and technology to protect customer data. In addition, financial services have long been subject to extensive privacy regulation. At the same time, this sector is recovering from the financial crisis the country has just gone through, and facing extensive new regulatory requirements under the Dodd-Frank Act. Thus, any new privacy recommendations should take into account the strong legal protections for financial information already in place and the importance of this sector's recovery to the nation's economy.

Since 1970, the FCRA has governed consumers' sensitive financial information. The FCRA promotes 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. FCRA applies to a number of different categories of persons and entities (depending on the particular provision of FCRA) -- not only to CRAs. For instance, under the FCRA, a person (whether an individual, a financial institution, or some other entity) may obtain a "consumer report" – such as a consumer credit report – from a CRA only in limited, specified circumstances where a "permissible purpose" for obtaining such a report exists and the person certifies that the person has such a permissible purpose. Any person that furnishes information about a consumer to a CRA also has numerous responsibilities, including participating in investigations regarding the accuracy of information the furnisher has reported about a consumer when the consumer has disputed such information. Any person that holds sensitive information about consumers must also ensure the proper disposal of such information when it is no longer needed. The FCRA Red Flags Rules requires financial institutions and certain other creditors to maintain identity theft prevention programs. The FCRA also places certain restrictions on the ability of any person to share and use consumer information among affiliates.

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 consumer 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.

Under the GLBA, consumer customers now must be provided with:

- Notice, annually, of the institution's practices regarding information collection, and disclosure, which must be clear, conspicuous, and updated to reflect changes to those practices;

- Opt-out choice regarding the institution's sharing of information with nonaffiliated third parties (unless any exception applies), and in certain instances, with affiliates;

- Security in the form of policies, procedures, systems, and controls to ensure that personal information remains confidential;

- Protection against most types of re-disclosure or re-use of personal information that is shared with third parties; and

- Enforcement of privacy protections via the full panoply of enforcement powers of financial institutions' regulatory agencies (the Securities and Exchange Commission, federal bank regulators, state insurance authorities, and the Federal Trade Commission). Federal regulatory authorities regularly examine financial institutions under their supervision for compliance with GLBA and FCRA (as well as with all other laws to which financial institutions are subject).

Moreover, the GLBA and its implementing regulations require financial institutions not only to limit the disclosure of consumer 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 where warranted.

The GLBA does not pre-empt state laws that are more protective of consumers. A number of U.S. states, including California, have enacted such laws, which tend to resemble GLBA but add additional protections, such as requiring a consumer customer's opt-in consent for certain types of information sharing.

Finally, U.S. regulations require SIFMA members to carefully select, contractually bind, and conduct ongoing monitoring of, third party service providers that receive personal data. In many cases, this process is subject to Federal Financial Institutions Examination Council guidance and monitoring procedures.

II. Fair Information Practices

Both the FTC and DOC reports recommend expansion of Fair Information Practice Principles (FIPPs). Whether or not the DHS FIPPS cited in the NTIA Green Paper, or the articulation of FIPPS in the FTC's staff report are appropriate for other, unregulated industry sectors, the financial services sector is already subject to robust fair information practices principles that are specifically tailored legal requirements applicable to financial services, and that have a clear track record of protecting the privacy and security of information about the industry's customers and consumers. Therefore, we urge both the DOC and the FTC to recognize that FIPPS cannot and should not be based on a "one size fits all" approach. Rather, any articulation of FIPPS must take into account existing requirements in the securities and financial services industries.

For instance, one of the proposed new FIPPs relates to the accuracy of information. Financial companies already have numerous, strong incentives to maintain highly accurate records which are the lifeblood of our industry. SIFMA members are regularly audited and examined by regulators to test the accuracy of records they maintain. The securities regulations place rigorous requirements on firms to maintain accurate customer account and other records. The FCRA imposes a duty of accuracy when members furnish information to consumer reporting agencies and the new Consumer Financial Protection Bureau has been given added authority to police accuracy. Most importantly, in order to maintain the confidence of its customers and remain viable entities, financial institutions must maintain accurate records. Customers would not stay long with a financial institution that did not maintain their accounts in proper order. Another proposed FIPP relates to data retention. This is yet another area that has long been addressed by regulations directed to the financial services industry. For example, securities firms are required to maintain customer account and other records for specified periods of time. Another example is the FCRA which contains an obsolescence period for reporting of negative information on consumers.

The United States has for decades embraced a sector-specific approach to privacy regulation. In fact, the DOC report notes that this sectoral approach "has facilitated innovation and spurred some of the world's most technologically advanced services, while also providing meaningful privacy protections." 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 privacy concepts to those industries is not only unnecessary, it could be inconsistent with existing regulations and produce unintended negative consequences. Therefore, consistent with the DOC approach or recommending "adoption of a comprehensive set of FIPPs to protect the privacy of personal information in commercial contexts *not covered by an existing sectoral law*," SIFMA recommends that the DOC's and FTC's final recommendations apply FIPPs only to companies not subject to sectoral laws that protect consumers.[2]

[2] DOC recommendation #8 likewise provides that "A baseline commercial data privacy framework should not conflict with the strong sectoral laws and policies that already provide important protections to Americans, but rather should act in concert with these protections." Since generally applicable FIPPs will inevitably conflict with the more specific sectoral laws, SIFMA recommends that any framework that is developed exclude industries where sectoral laws apply.

III. Privacy by Design

The FTC has proposed that companies should promote privacy throughout their organizations and at every stage of the development of products and services. This is not a new concept to the financial services industry which has long had to consider privacy regulations during the development stages of new products and services. It is important that any new privacy by design process be forward looking. While existing products and services have been built to comply with applicable law, it can be extremely costly and burdensome, and in some cases impossible, to retrofit them.

There is still a role that the federal government could play in helping companies' improve their internal processes. Some companies may develop innovate approaches to incorporating privacy into the design process but there is no easy way to share these innovations. This highlights a synergy between the FTC and DOC reports: the FTC has proposed a process for designing-in privacy and DOC has suggested a way to improve it. The DOC's proposed Privacy Policy Office (PPO) could serve as a center of commercial data privacy expertise. In doing so, it could help make companies aware of best practices as they develop by acting as a clearinghouse. As DOC has proposed, the "PPO would have the authority to convene multi-stakeholder discussions of commercial data privacy implementation models, best practices, codes of conduct, and other areas that would benefit from bringing stakeholders together." Not only would this benefit industry, it would also enhance the PPO's knowledge of privacy issues best practices and challenges, improving its ability to develop privacy policy recommendations.

IV. Simplified Consumer Choice

The FTC proposes simplifying the consumer choice process regarding how personal information is used. The financial services industry is leading the pack on this with the new interagency model privacy notices that became available for use this year. While adoption of the model format is optional, some major financial institutions have already started to use it and others are sure to follow. No other U.S. industry is now employing such easy to read and understand privacy notice. In fact, these model notices are serving as a test of the FTC's proposed approach, namely whether consumers are more likely to read and find useful simplified notices. Over time, we will find out whether this alternative to the previous sometimes wordy privacy notices will be an effective way to communicate with consumers.

While simplified notices can be very helpful, we are concerned with the part of the FTC's proposal that offers consumers' choice at a time and in a context in which the consumer is making his or her decision to provide information is unworkable. First, we believe a clearly articulated privacy notice, such as the model notice, makes this process unnecessary, as consumers will have a full understanding of how their information will be used and disclosed from the outset. Second, imposing additional notice and choice every time a consumer enters into even routine transaction is likely to burden those consumers who are anxious to complete a transaction. This added step for every transaction is unlikely to result in better decisions about how those consumers' information will be used. In fact, consumers intent on making a deposit, ordering a trade, or cashing a check are unlikely to want to read privacy notices and have to click on even more boxes to complete their business. If the FTC believes that certain information uses and/or disclosures require this type of notice and/or consent, the FTC should specify exactly what those are to avoid any uncertainty. It should then seek public comment on

the list before finalizing its report. In any event, this proposal is premature until the new model privacy notices are given a chance in the marketplace.

V. Consumer Education

The FTC calls on companies to accelerate efforts to raise consumer awareness about data practices and to provide additional transparency tools to consumers, noting that consumers lack understanding of various data practices and their privacy implications, and thus lack the ability to make informed decisions about the trade-offs involved. Increased consumer education – in conjunction with the clearer and stronger protections discussed above – will help alleviate these concerns. In addition, the Commission staff requests input on how individual businesses, industry associations, consumer groups, and government can do a better job of informing consumers about privacy.

SIFMA believes that educating consumers about the importance of understanding companies' data practices and their privacy implications is vital. Under the GLBA, financial institutions are required to provide consumers an initial and annual privacy notice informing consumers about what information is collected and disclosed to affiliates and third parties, and opportunities of consumers to opt out of certain such disclosures. SIFMA believes this should be part of a larger effort to also educate consumers about how to protect their sensitive personal information and techniques they can use to prevent becoming victims of identity theft. Such a campaign could address proper disposal of computers that may contain personal information; how to prevent or detect spyware that intruders may have installed on their computers; how to avoid becoming a victim of pretexting, phishing and pharming scams; and what steps to take if the consumer has become a victim of identity theft.

VI. Voluntary Enforceable Codes of Conduct

A centerpiece of the DOC report is encouraging the development of voluntary, enforceable codes of conduct as a mechanism for assuring privacy protections. While voluntary, these codes would be enforceable by the FTC because they would constitute "representations" and failure to comply with them could be considered a deceptive trade practice under the FTC Act.

A hallmark of the securities industry has been its longstanding commitment to self-regulation. The Financial Industry Regulatory Authority (FINRA) is the largest independent regulator for all securities firms doing business in the United States. FINRA's mission is to protect America's investors by making sure the securities industry operates fairly and honestly. FINRA oversees nearly 4,580 brokerage firms, about 162,850 branch offices and approximately 630,695 registered securities representatives.

Furthermore, FINRA touches virtually every aspect of the securities business—from registering and educating industry participants to examining securities firms; writing rules; enforcing those rules and the federal securities laws; informing and educating the investing public; providing trade reporting and other industry utilities; and administering the largest dispute resolution forum for investors and registered firms. It also performs market regulation under contract for the major U.S. stock markets, including the New York Stock Exchange, NYSE Arca, NYSE Amex, The NASDAQ Stock Market and the International Securities Exchange. FINRA has

approximately 3,000 employees and operates from Washington, DC, and New York, NY, with 20 regional offices around the country.

Once again, the financial services industry is ahead of the curve on protecting consumers' privacy. With a robust, self-regulatory organization in place, we do not see the need to develop new structures or codes of conduct to appropriately address protection of consumers' privacy. If a code was nonetheless determined to be appropriate, it should be sector specific taking into account the unique attributes of financial services.

VII. Security Breach Notification

The DOC has suggested that consideration be given to adoption of a federal comprehensive commercial data security breach framework for electronic records that includes notification provisions, encourages companies to implement strict data security protocols. SIFMA believes that a national breach notification requirement should be adopted. A standard that links an obligation to notify consumers in the event of a breach with the crime of identity theft is appropriate. Any notification threshold should be tied to an actual threat to the consumer to which he or she might reasonably and effectively be expected to respond. We also believe that functional regulators like the SEC are best suited to monitor industry compliance. Therefore, we make the following recommendations:

A. Uniform National Standards

Almost every state has enacted security breach legislation that requires disclosure of a breach of security of a computer system to the person whose sensitive personal information was compromised. Legislative requirements often vary from state to state. Such differences result in a patchwork of laws that are difficult to comply with and which often conflict. More importantly, the multitude of state and local laws is likely to result in confusion and potential harm to consumers. Consumers in different states could be subject to different security standards and levels of notification despite the fact that the harm they may suffer as a result of a security breach at the same institution is identical. For these reasons, SIFMA urges the DOC to recommend legislation that results in a uniform national standard that pre-empts state laws.

B. Harm Trigger

SIFMA believes that any national security breach notification requirement provide that consumers need only be notified when there is a significant risk that they will become victims of identity theft. Requiring notification if there is no significant risk of identity theft could have the unanticipated effect of overwhelming consumers with notices that might cause confusion and likely desensitize them to future notices. SIFMA believes that linking the notice requirement to a determination by the company, after reasonable investigation, that there is a significant risk that the consumer will become a victim of identity theft, strikes the appropriate balance for both consumers and financial institutions alike.

C. Sensitive Personal Information

SIFMA believes that notice to consumers should be required only in connection with a breach involving the kind of information that could be used to commit identity theft, such as

unencrypted or unredacted sensitive personal information that can be used directly to commit identity theft or to access an individual's financial accounts. This is the only type of information that most likely can be used to perpetrate identity theft. There is little reason to require notification be sent to consumers when the information obtained is of little or no practical value to an identity thief.

D. Functional Regulator Oversight and Rulemaking

Given the existing regulatory framework of the GLBA and the expertise of functional regulators in addressing identity theft and data security, SIFMA believes that DOC should recognize in its recommendations to Congress the primary role of functional regulators in addressing these issues and support granting them exclusive rulemaking and oversight authority. Functional regulators examine institutions for compliance and possess authority to sanction those not in compliance. Accordingly, we recommend that DOC's recommendations addressing the security of data held by securities firms and other financial institutions subject to the GLB Act should provide that the functional regulators have the exclusive authority to develop and enforce regulations affecting institutions subject to their jurisdiction.

VIII. International Leadership

While SIFMA applauds the DOC's recognition of the importance of providing international advocacy on behalf of the U.S. approach to privacy protection, we urge the Department to ensure that such advocacy includes and promotes mutual recognition for sector-specific laws, regulations, and FIPPs. As other countries and geographic regions develop privacy protection approaches, they are often general and do not take into account the unique aspects of certain economic sectors, such as financial services, or existing protections for those sectors under national laws, such as the U.S. laws discussed above. We hope that in such discussions, DOC will resist application of such general principles to economic sectors where privacy protections already exist.

IX. ECPA Reform

There is unquestionably a need to update the Electronic Communications Privacy Act ("ECPA". That law, enacted in 1986, makes assumptions about a static technology marketplace that bears little resemblance to the way in which individuals communicate, interact, and engage on the Internet in 2011. For example, ECPA affords lesser protections to email communications based on where messages are stored, whether messages have been opened, and how long messages have existed. As a result, there is legal uncertainty about cloud computing. Domestically, the rules applicable to data stored in the cloud must be predictable if emerging distributed computing technology is to achieve its potential, as the absence of such predictability erodes consumer confidence and drives up costs for businesses. In addition, the lack of clarity can and is being used internationally to disadvantage U.S. businesses, including financial services, using or providing cloud computing services. In the financial services sector as in other industry sectors, information technology has driven the U.S. economy for decades and likely to drive economic growth for the foreseeable future.[3]

---

[3] *See* Robert D. Atkinson & Andrew S. McKay, *Information Technology & Innovation Foundation, Digital Prosperity: Understanding the Economic Benefits of the Information Technology Revolution,* at 11-14 (March 2007).

* * *

SIFMA appreciates your consideration of our views and concerns on the reports. If you have any questions, please call me at 202-962-7385.

Respectfully submitted,

/Melissa MacGregor/

Melissa MacGregor
Managing Director and Associate General Counsel

cc: David Medine, WilmerHale