

# THE FINANCIAL SERVICES ROUNDTABLE



1001 PENNSYLVANIA AVE., NW  
SUITE 500 SOUTH  
WASHINGTON, DC 20004  
TEL 202-289-4322  
FAX 202-628-2507

## BITS

FINANCIAL SERVICES  
R O U N D T A B L E

May 12, 2008

Send via email: [rule-comments@sec.gov](mailto:rule-comments@sec.gov)

Nancy M. Morris  
Office of the Secretary  
Securities and Exchange Commission  
100 F Street, NE  
Washington, DC 20549

Re: SEC Proposed Amendments to Regulation S-P, File Number S7-06-08

Dear Sirs and Madams:

The Financial Services Roundtable, including BITS, (“Roundtable”) appreciates the opportunity to comment to the Securities and Exchange Commission (“SEC”) on the proposals set forth in “Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information”.<sup>1</sup> Our members recognize data security risks and have taken active steps individually and in collaboration with others through participation in BITS and the Identity Theft Assistance Center (ITAC) to address these risks.<sup>2</sup> Financial institutions have a strong history of protecting customer information, deploying broadly accepted authentication methods, applying security controls to detect and prevent fraudulent activities, and educating customers on how to protect their information and prevent identity theft. Customer trust in the security and continuity of financial transactions is vital to the stability of the industry and the strength of the nation’s economy. Our member financial institutions work diligently to maintain that trust as they continually improve their technologies, processes and procedures to protect customers’ information.

Overall, we urge the SEC to:

- Harmonize the amendments to S-P with the regulations issued by the Federal Banking Agencies except where there are compelling reasons not to do so;

---

<sup>1</sup> The Financial Services Roundtable represents 100 of the largest integrated financial services companies providing banking, insurance, investment products and services to the American consumer. Roundtable member companies provide fuel for America’s economic engine accounting directly for \$66.1 trillion in managed assets, \$1.1 trillion in revenue and 2.5 million jobs. BITS is a division of the Roundtable, leveraging intellectual capital to address issues at the intersection of financial services, operations and technology. BITS focuses on strategic issues where industry cooperation serves the public good, such as fraud prevention, critical infrastructure protection, and the safety of financial services.

<sup>2</sup> The Identity Theft Assistance Center (“ITAC”), another division of The Roundtable, fights identity theft by helping victims recover from this serious crime, partnering with law enforcement to catch and convict criminals, and conducting research on the causes of and solutions to identity theft. The ITAC provides a free victim assistance service to customers of member companies.

- Apply consistent definitions to key terms such as “personal information” and refrain from expanding the scope beyond consumer customer information;
- Not adopt a standard form as proposed with SP-30 and thus grant greater flexibility in determining when to notify regulators and the method of notification;
- Adopt a more flexible rule governing the disposal of documents that would permit entities to periodically review and document in writing their disposal practices to verify there is compliance with the company's policies and procedures; and
- Provide for at least a 12 month implementation period after publication of the final rule.

## Harmonization of Requirements

In general, the Roundtable appreciates and supports efforts by the Commission to enact rules that are consistent with existing privacy and information security regulations from the Federal Banking Agencies. The Roundtable is supportive of an approach that is more principles based than it is prescriptive. Greater consistency in rules will help integrated financial services companies better serve their customers and reduce compliance costs. Many of our member companies are securities firms with affiliated banking organizations and vice versa. These companies have implemented information security and breach notification programs that comply with the Federal Banking Agency rules and FFEIC guidance. Harmonization of requirements will enable securities firms to comply more effectively and more efficiently with uniform standards adopted by all the Federal Banking Agencies. Imposing standards in Regulation S-P that are inconsistent with those applicable to banking organizations would be unduly and unnecessarily burdensome for many securities firms.

We believe that the Commission’s proposed amendments are a step in the right direction for meeting the objectives of Section 501 of the Gramm-Leach-Bliley Act (“GLBA”). Most of the proposed changes are consistent with existing regulations from the Federal Banking Agencies; however, there are several proposed changes outlined below where we comment on inconsistencies that could raise issues for financial institutions under the Commission’s jurisdiction.<sup>3</sup> We urge the SEC to carefully examine the proposed regulation to ensure that it does not unnecessarily increase regulatory burdens associated with the GLBA and existing Federal Banking Agency requirements. Furthermore, the Roundtable is concerned with the potential confusion that may result from the growing proliferation of data protection-related regulatory requirements. In addition to the requirements of existing banking regulatory guidance related to the GLBA, additional areas of guidance such as the final rules implementing the Fair and Accurate Credit Transactions Act’s (FACTA) identity theft “red flags” rule, are creating a growing body of specific requirements with which financial institutions must comply. In addition to these regulations, the Federal Banking Agencies have issued supervisory guidance ranging from authentication to oversight of third party providers through the Federal Financial Institutions Examination Council (FFIEC). While many of our securities companies and integrated financial services companies pay close attention to FFIEC guidance, we do not believe it is necessary or practical for the SEC to incorporate all of these in the amendments to Regulation S-P.

---

<sup>3</sup> The Roundtable submitted a comment on the proposed breach rules issued by the Federal Banking Agencies in 2003. This letter can be found at: <http://www.bitsinfo.org/downloads/Comment%20letters/bitsbreachnotcloct03.pdf>. BITS and the American Bankers Association (ABA) completed the *BITS/ABA Key Considerations for Responding to Unauthorized Access to Sensitive Customer Information* in 2006 to help financial institutions develop and execute response programs when confidential and sensitive information is accessed or misused by unauthorized individuals. The paper covers the evolving legal and regulatory requirements, potential elements of a response program, and suggestions for managing third party service provider relationships as they relate to data security programs and customer notification.

## **Designation of Responsible Employee**

Our members agree that institutions subject to Regulation S-P should be required to designate an employee, or employees, to coordinate their information security program. We also request that the SEC permit securities firms that are part of diversified financial services organizations to designate an employee of an affiliate, or a position at an affiliate, as the person responsible for coordinating the securities firm's information security program. Such flexibility will help ensure that the policies and procedures of such firms are consistent and coordinated throughout the organization as a whole.

## **Key Definitions**

Some of the definitions included within this proposed rule are not consistent with other financial privacy and security regulations and the underlying statutes. We urge the Commission to apply the same definitions as the Federal Banking Agencies unless the SEC provides a compelling reason not to do so. Leveraging the financial privacy and security regulations and best practices that have been used for several years will ensure a successful transition and will reduce compliance costs, especially for integrated financial services firms.

### *Sensitive Personal Information*

The amendments to Regulation S-P define "sensitive personal information" as "any personal information, or any combination of components of personal information, that would allow an unauthorized person to use, log into, or access an individual's account, or to establish a new account using the individual's identifying information, including the individual's Social Security Number, or any one of the individual's names, telephone numbers, street address, e-mail address, or online user name, in combination with any one of the individual's account numbers, credit or debit card numbers, driver's license number, credit card expiration date or security code, mother's maiden name, password, PIN number, biometric authentication record, or other authenticating information." This definition of "sensitive personal information" is much broader than the definition of sensitive customer information used in GLBA and in existing requirements of the Federal Banking Agencies.<sup>4</sup> The proposed definition includes both consumer report information and nonpublic personal information.<sup>5</sup> Consequently, the construction of the Commission's proposed definition of "sensitive personal information" will encompass virtually all information about an individual. We urge the Commission to refrain from expanding the scope of sensitive personal information beyond consumer customer information, which is the standard authorized under Section 501 of the GLBA.

The Commission's proposed designation of Social Security Numbers ("SSNs") by themselves as sensitive personal information is inconsistent with existing regulation. Existing guidance only stipulates SSNs as Personally Identifiable Information ("PII") if included in conjunction with other information. In September 2007, the Roundtable submitted a comment letter in response to an FTC request for information on private sector use of SSNs. That letter reviewed the required uses of SSNs and challenges

---

<sup>4</sup> The Banking Regulatory Agencies define *sensitive customer information* as a customer's name, address, or telephone number, in conjunction with the customer's social security number, driver's license number, account number, credit or debit card number, or a personal identification number or password that would permit access to the customer's 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 or password and account number.

<sup>5</sup> The current Reg. S-P defines "nonpublic personal information" to include information from a consumer report. (248.3(t)(1)(i) and (u)(1)(G)).

in trying to restrict its use in customer identification.<sup>6</sup> Additionally, we urge the SEC to exclude the mother's maiden name from the definition of "sensitive personal information."

We are concerned that the designation of an employee's information for the Information Security Program goes beyond Section 501 of GLBA. We believe that "personal information" should be limited to customers and not include employees and non-natural persons. Existing banking regulation does not currently apply to a company's employees, only its customers. If the SEC intends to include employee authentication for accessing customer information, the SEC should note that directly and define employee information more narrowly. Additionally, "personal information" should not include investors or security holders, unless they are customers.

#### *Substantial Harm or Inconvenience*

"Substantial harm or inconvenience" is defined in the proposed amendments as "personal injury, or more than trivial financial loss, expenditure of effort or loss of time." The Roundtable is concerned that there is a wide gap between "trivial" and "substantial" and thus would treat any financial loss that is slightly above "trivial" as "substantial." Furthermore, this definition is not consistent with the standard adopted by the Federal Banking Agencies. Unless the SEC provides a compelling reason not to do so, we suggest that the SEC apply the same standard of the banking agencies. This standard has provided adequate protection for consumers and is well understood by the industry. We also urge the SEC to state in the final rule that if financial institutions can demonstrate that breached data is rendered unusable (e.g., effective use of encryption technology, other technologies or controls) it should not be defined as causing substantial harm or inconvenience. Furthermore, there are numerous examples of situations where there is no substantial harm or inconvenience, including unintentional mailing of an account statement to an incorrect address, access by employees of affiliates and service providers, and "good faith acquisition" of personal information by such parties. The SEC should acknowledge these examples in its final rule.

#### *Service Provider*

In the proposed amendments, the term "service provider" is defined as "any person or entity that receives, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a person subject to the rule." We urge the SEC to amend the definition so that it excludes internal, affiliated companies.

#### **Information Security Program and Data Security Breach Response**

In general, the proposed amendments to Regulation S-P would require more specific information security and breach notification standards which are more consistent with the approach of the Federal Banking Agencies. We strongly support efforts to achieve greater consistency. Moreover, the SEC proposes that such "information security programs" include procedures for responding to incidents of unauthorized access to or use of personal information. Procedures would include: notice to affected individuals if misuse of sensitive personal information has occurred or is reasonably possible; and notice to the SEC or designated examining authority under circumstances in which an individual identified with the information has suffered substantial harm or inconvenience, or an unauthorized person has intentionally obtained access to or used sensitive personal information. Our members support the "harm trigger" clause and threshold of "significant risk." We also urge the SEC to explicitly recognize that one or more entities

---

<sup>6</sup> [http://www.fsround.org/policy/regulatory/pdfs/FSRoundtablecomments\\_SSNs\\_090507.pdf](http://www.fsround.org/policy/regulatory/pdfs/FSRoundtablecomments_SSNs_090507.pdf)

subject to SEC jurisdiction may be covered by the information security program of a parent company which also encompasses non-SEC entities.

### **Notice and Form SP-30**

The proposed rule requires broker-dealers to provide written notice to their designated examining authority on a proposed form SP-30 as soon as possible after becoming aware of an incident of unauthorized access to, or use of, personal information in which there is a significant risk of substantial harm or inconvenience to the individual, or an unauthorized person has intentionally obtained access to or used sensitive personal information. We believe the appropriate threshold for determining when to notify the Commission should be limited to circumstances where an individual has suffered “substantial harm or inconvenience.” We believe there is no compelling reason to require notice to regulators if an unauthorized person has obtained access to or used sensitive personal information but there is no significant risk of harm or inconvenience to the individual. Such a requirement would be an unnecessary burden for financial institutions, and would be costly to observe.

We recommend that the SEC not adopt the proposed form SP-30 for several reasons. First, the Federal Banking Agencies do not require financial institutions to use a specific form or method of notice. Second, the proposed form requires specific information that is generally not available at the time of discovery of a breach. Third, a mandate for this level of specific reporting may impede effective reporting of incidents to the SEC. If, however, the SEC believes that such a form is necessary, we urge the Commission to develop a far less specific, more general form for reporting incidents. We also urge the SEC to treat filed reports as confidential information similar to the way Suspicious Activity Reports are treated.

The proposed rule contemplates that broker-dealers should provide written notice to their designated examining authority (“DEA”) on Form SP-30 under more limited circumstances than the notice to customers. In fact, the release makes clear the intention of the Commission to “avoid notice to the [DEA] in every case of unauthorized access, and to focus scrutiny on information security breaches that present a greater likelihood of potential harm,” (*Release, 73 Fed. Reg. 13698*). However, despite the clear intention of the Commission in the release, the actual language of the proposed rule requires notice to the firm’s DEA not only where there is (A) a significant risk of substantial harm or inconvenience to the individual but also where (B) *an unauthorized person has intentionally obtained access to or used sensitive personal information*, Section 248.30(4)(v)(A) and (B). In order to provide clarity regarding the standard for reporting breaches to individuals and pursuant to Form SP-30, the SEC should consider reconciling the inconsistent standards being applied in Section 248.30(4) by striking Section 248.30(4)(v)(B).

We do not believe the SEC should establish a specific threshold regarding the number of affected individuals in determining when to notify the SEC or affected customers following the discovery of a breach.

We urge the SEC to clarify what is meant by “as soon as possible” by applying the standard in most breach laws – “without unreasonable delay.” Based on the experience over the past several years, breaches vary significantly and each requires an analysis of the mitigating controls to determine whether the breached data is unusable and thus whether consumers are truly at risk of harm. The harm standards are important guidance which would help ensure that needless over-reporting or under-reporting is avoided.

### **Safeguards and Disposal Rule Requirement**

The proposed rule expands the current Commission rule regarding the disposal of personal information by requiring firms to document in writing their proper disposal of personal information. Unless clarified, this could be interpreted as requiring a written record every time a firm disposes of any personal information. This would be a significant and unnecessary burden on firms given that other parts of the proposal that broaden the disposal rule to include natural persons. Our members believe that firms should not be required to document every disposal of documents containing personal information. Instead, we recommend proposing an alternative to Sec. 248.30(b)(2)(ii) that would require regulated entities to “periodically review and document in writing their disposal practices to verify there is compliance with the company’s policies and procedures.” This would provide for verification that disposal policies are actually being applied, yet not overburden the company and registered representatives with record keeping.

### **Service Provider Assessment Tools**

The SEC identified several tools used to ensure effective security controls for service providers of financial institutions that included: Web Trust, SAS 70, and Systrust. We prefer that if the SEC plans to identify examples of effective tools in use today to assess information security controls for service vendors, that it includes the BITS Shared Assessments Program in the examples. The BITS Shared Assessments Program is a codified practice of security assurance designed specifically for financial institutions to assess the effectiveness of core security controls for service vendors. The program was initiated because of dissatisfaction with both the depth and efficiency of existing alternative assessment tools for third party service providers.<sup>7</sup>

### **Departing Representatives**

The SEC proposes a new exception from Regulation S-P’s notice and opt-out requirements to allow investors more easily to follow a representative who moves from one brokerage or advisory firm to another. Our members are divided on this provision. Some members are opposed to it and believe it violates GLBA while others recommend that this aspect of the proposal be amended to permit such transfer of information, provided both the individuals’ prior firm, and their new firm agrees to the transfer.

### **Compliance Date**

Due to the complexity of the proposal, the Roundtable once again recommends that the SEC should re-evaluate this proposal to make it consistent with current laws and regulations within the financial services industry. Once that review is accomplished, the Roundtable recommends that the SEC include a compliance date of at least a year from the rule’s effective date.

### **Conclusion**

The Roundtable appreciates the efforts of the SEC to propose amendments to Regulation S-P that are generally consistent with existing regulation from the Federal Banking Agencies. We urge the Commission to consider our comments concerning consistency in key definitions and refraining from

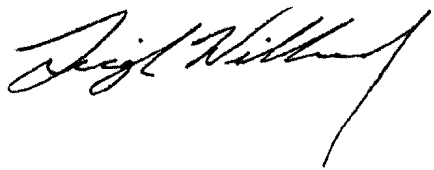
---

<sup>7</sup> For information on the BITS Shared Assessments Program see: <http://www.bitsinfo.org/FISAP/index.php>.

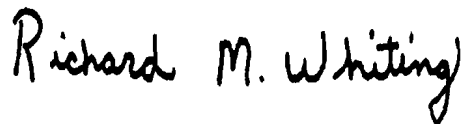
expanding the scope beyond consumer customer information. We urge the Commission to not adopt proposed SP-30 and grant flexibility in determining when to notify regulators and the method of notification. We also urge the Commission to adopt a more flexible disposal of documents requirement that would permit entities to periodically review and document in writing their disposal practices to verify there is compliance with the company's policies and procedures. Finally, we urge the Commission to provide for at least a 12 month implementation period after publication of the final rule.

Thank you for your consideration. If you have any further questions or comments on this matter, please do not hesitate to contact us, John Carlson, Senior Vice President of BITS, or Melissa Netram, Director, Regulatory and Securities Affairs, The Financial Services Roundtable, at (202) 289-4322.

Sincerely,



Leigh Williams  
President  
BITS



Richard M. Whiting  
Executive Director and General Counsel  
The Financial Services Roundtable