SECURITIES AND EXCHANGE COMMISSION

17 CFR Part 248

[Release Nos. 34–57427; IC–28178; IA–2712; File No. S7–06–08]

RIN 3235–AK08

Part 248—Regulation S–P: Privacy of Consumer Financial Information and Safeguarding Personal Information

AGENCY: Securities and Exchange Commission.

ACTION: Proposed rule.

SUMMARY: The Securities and Exchange Commission (''Commission'') is proposing amendments to Regulation S–P, which implements certain provisions of the Gramm-Leach-Bliley Act (''GLBA'') and the Fair Credit Reporting Act (''FCRA'') for entities regulated by the Commission. The proposed amendments would set forth more specific requirements for safeguarding information and responding to information security breaches, and broaden the scope of the information covered by Regulation S–P's safeguarding and disposal provisions. They also would extend the application of the disposal provisions to natural persons associated with brokers, dealers, investment advisers registered with the Commission (''registered investment advisers'') and transfer agents registered with the Commission (''registered transfer agents''), and would extend the application of the safeguarding provisions to registered transfer agents. Finally, the proposed amendments would permit a limited transfer of information to a nonaffiliated third party without the required notice and opt out when personnel move from one broker-dealer or registered investment adviser to another.

DATES: Comments must be received on or before May 12, 2008.

ADDRESSES: Comments may be submitted by any of the following methods:

Electronic Comments

- Use the Commission's Internet comment form (*http://www.sec.gov/rules/proposed.shtml*); or
- Send an e-mail to *rule-comments@sec.gov.* Please include File Number S7–06–08 on the subject line; or
- Use the Federal eRulemaking Portal (*http://www.regulations.gov*). Follow the instructions for submitting comments.

Paper Comments

- Send paper comments in triplicate to Nancy M. Morris, Secretary, Securities and Exchange Commission, 100 F Street, NE., Washington, DC 20549–1090.

All submissions should refer to File Number S7–06–08. This file number should be included on the subject line if e-mail is used. To help us process and review your comments more efficiently, please use only one method. The Commission will post all comments on the Commission's Internet Web site (*http://www.sec.gov/rules/proposed.shtml*). Comments are also available for public inspection and copying in the Commission's Public Reference Room, 100 F Street, NE., Washington, DC 20549, on official business days between the hours of 10 a.m. and 3 p.m. All comments received will be posted without change; we do not edit personal identifying information from submissions. You should submit only information that you wish to make available publicly.

FOR FURTHER INFORMATION CONTACT: Catherine McGuire, Chief Counsel, or Brice Prince, Special Counsel, Office of the Chief Counsel, Division of Trading and Markets, (202) 551–5550; or Penelope Saltzman, Acting Assistant Director, or Vincent Meehan, Senior Counsel, Office of Regulatory Policy, Division of Investment Management, (202) 551–6792, Securities and Exchange Commission, 100 F Street, NE., Washington, DC 20549.

SUPPLEMENTARY INFORMATION: The Commission today is proposing amendments to Regulation S–P [1] under Title V of the GLBA,[2] the FCRA,[3] the Securities Exchange Act of 1934 (the ''Exchange Act''),[4] the Investment Company Act of 1940 (the ''Investment Company Act''),[5] and the Investment Advisers Act of 1940 (the ''Investment Advisers Act'').[6]

Table of Contents

I. Background

A. Statutory Requirements and Current Regulation S–P Mandates

Subtitle A of Title V of the GLBA requires every financial institution to inform its customers about its privacy policies and practices, and limits the circumstances in which a financial institution may disclose nonpublic personal information about a consumer to a nonaffiliated third party without first giving the consumer an opportunity to opt out of the disclosure.[7] In enacting the legislation, Congress also specifically directed the Commission and other federal financial regulators to establish and implement information safeguarding standards requiring financial institutions subject to their jurisdiction to adopt administrative, technical and physical information safeguards.[8] The GLBA specified that these standards were to ''insure the

[1] 17 CFR part 248. Unless otherwise noted, all references to rules under Regulation S–P will be to Part 248 of the Code of Federal Regulations (17 CFR 248).

[2] 15 U.S.C. 6801–6827.

[3] 15 U.S.C. 1681w.

[4] 15 U.S.C. 78a.

[5] 15 U.S.C. 80a.

[6] 15 U.S.C. 80b.

[7] *See* 15 U.S.C. 6802(a) and (b). The GLBA and Regulation S–P draw a distinction between ''consumers'' and ''customers.'' A ''consumer'' is defined in Section 3(g)(1) of Regulation S–P to mean an individual who obtains a financial product or service that is to be used primarily for personal, family, or household purposes. *See* 17 CFR 248.3(g)(1). A ''customer'' is defined in Section 3(j) of Regulation S–P as a consumer who has a continuing relationship with the financial institution. *See* 17 CFR 248.3(j). The distinction between customer and consumer determines the notices that a financial institution must provide. Pursuant to Sections 4 and 5 of Regulation S–P, a financial institution must provide *customers* with an initial notice describing the institution's privacy policies when a customer relationship is formed and at least annually throughout the customer relationship. In contrast, if a *consumer* is not a customer, a financial institution must only provide a notice if it intends to share nonpublic personal information about the consumer with a nonaffiliated third party (outside of certain exceptions). *See* 17 CFR 248.4 and 248.5.

[8] The GLBA directed the Commission, the Federal Trade Commission (''FTC'') and state insurance authorities to implement the safeguarding standards by rule. *See* 15 U.S.C. 6805(b)(2). The GLBA directed the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation (''FDIC'') and the Office of Thrift Supervision (collectively, the ''Banking Agencies'') and the National Credit Union Administration (''NCUA'') to implement the safeguarding standards by regulation or by guidelines. *See* 15 U.S.C. 6805(b)(1).

security and confidentiality of customer records and information,'' ''protect against any anticipated threats or hazards to the security or integrity'' of those records, and protect against unauthorized access to or use of those records or information, which ''could result in substantial harm or inconvenience to any customer.'' [9]

In response to these directives, we adopted Regulation S–P in 2000.[10] Section 30(a) of Regulation S–P (the ''safeguards rule'') requires institutions to safeguard customer records and information,[11] while other sections of the regulation implement the notice and opt out provisions of the GLBA.[12] The safeguards rule currently requires institutions to adopt written policies and procedures for administrative, technical, and physical safeguards to protect customer records and information. The safeguards must be reasonably designed to meet the GLBA's objectives.[13] This approach provides flexibility for institutions to safeguard customer records and information in accordance with their own privacy policies and practices and business models. The safeguards rule and the notice and opt out provisions currently apply to brokers, dealers, registered investment advisers, and investment companies.[14]

Pursuant to the Fair and Accurate Credit Transactions Act of 2003 (''FACT Act''), the Commission amended Regulation S–P in 2004 to protect against the improper disposal of consumer report information.[15] Section 30(b) of Regulation S–P (the ''disposal rule'') currently applies to the institutions subject to the other provisions of Regulation S–P, except that it excludes notice-registered broker-dealers and includes registered transfer agents.

B. Challenges Posed by Information Security Breaches

In recent years, we have become concerned with the increasing number of information security breaches that have come to light and the potential for identity theft and other misuse of personal financial information. Once seemingly confined mainly to commercial banks and retailers, this problem has spread throughout the business community, including the securities industry.[16]

In the last two years, we have seen a significant increase in information security breaches involving institutions we regulate. Perhaps most disturbing is the increase in incidents involving the takeover of online brokerage accounts, including the use of the accounts by foreign nationals as part of ''pump-and-dump'' schemes.[17] The financial

[9] 15 U.S.C. 6801(b).

[10] *See Privacy of Consumer Financial Information (Regulation S–P)*, Exchange Act Release No. 42974, Investment Company Act (''ICA'') Release No. 24543, Investment Advisers Act (''IAA'') Release No. 1883 (June 22, 2000), 65 FR 40334 (June 29, 2000). Pursuant to the GLBA directive, Regulation S–P is consistent with and comparable to the financial privacy rules adopted by other federal financial regulators in 2000. *See* FTC, *Privacy of Consumer Financial Information*, 65 FR 33646 (May 24, 2000); Banking Agencies, *Privacy of Consumer Financial Information*, 65 FR 35162 (June 1, 2000); and NCUA, *Privacy of Consumer Financial Information; Requirements for Insurance*, 65 FR 31722 (May 18, 2000). *See also* 15 U.S.C. 6804(a)(2) (directing federal financial regulators to consult and coordinate to assure, to the extent possible, that each agency's regulations are consistent and comparable with the regulations prescribed by the other agencies).

In 2001, we amended Regulation S–P to permit futures commission merchants and introducing brokers that are registered by notice as broker-dealers in order to conduct business in security futures products under Section 15(b)(11)(A) of the Exchange Act (''notice-registered broker-dealers'') to comply with Regulation S–P by complying with financial privacy rules that the Commodity Futures Trading Commission (''CFTC'') adopted that year. *See* 17 CFR 248.2(b); *Registration of Broker-Dealers Pursuant to Section 15(b)(11) of the Securities Exchange Act of 1934*, Exchange Act Release No. 44730 (Aug. 21, 2001), 66 FR 45138 (Aug. 27, 2001); *see also* CFTC, *Privacy of Consumer Financial Information*, 66 FR 21236 (Apr. 27, 2001).

[11] 17 CFR 248.30(a).

[12] *See* 17 CFR 248.1–248.18. As described above, the GLBA and Regulation S–P require brokers, dealers, investment advisers registered with the Commission, and investment companies to provide an annual notice of their privacy policies and practices to their customers (and notice to consumers before sharing their nonpublic personal information with nonaffiliated third parties outside certain exceptions). *See supra* note 7; 15 U.S.C. 6803(a); 17 CFR 248.4; 17 CFR 248.5. In general, the privacy notices must describe the institutions' policies and practices with respect to disclosing nonpublic personal information about a consumer to both affiliated and nonaffiliated third parties. 15 U.S.C. 6803; 17 CFR 248.6. The notices also must provide a consumer a reasonable opportunity to direct the institution generally not to share nonpublic personal information about the consumer (that is, to ''opt out'') with nonaffiliated third parties. 15 U.S.C. 6802(b); 17 CFR 248.7. (The privacy notice also must provide, where applicable under the FCRA, a notice and an opportunity for a consumer to opt out of certain information sharing among affiliates.) Sections 13, 14, and 15 of Regulation S–P (17 CFR 248.13, 17 CFR 248.14, and 17 CFR 248.15) set out exceptions from these general notice and opt out requirements under the GLBA. Section 13 includes exceptions for sharing information with other financial institutions under joint marketing agreements and with certain service providers. Section 14 includes exceptions for sharing information for everyday business purposes, such as maintaining or servicing accounts. Section 15 includes exceptions for disclosures made with the consent or at the direction of a consumer, disclosures for particular purposes such as protecting against fraud, disclosures to consumer reporting agencies, and disclosures to law enforcement agencies. In March 2007, the Commission, together with the Banking Agencies, the CFTC, the FTC, and the NCUA, published for public comment in the **Federal Register** a proposed model privacy form that financial institutions could use for their privacy notices to consumers required by the GLBA. *See Interagency Proposal for Model Privacy Form Under the Gramm-Leach-Bliley Act*, Exchange Act Release No. 55497, IAA Release No. 2598, ICA Release No. 27755 (Mar. 20, 2007), 72 FR 14940 (Mar. 29, 2007) (''Interagency Model Privacy Form Proposal'').

[13] Specifically, the safeguards must be reasonably designed to insure the security and confidentiality of customer records and information, protect against anticipated threats to the security or integrity of those records and information, and protect against unauthorized access to or use of such records or information that could result in substantial harm or inconvenience to any customer. *See supra* note 9 and accompanying text.

[14] Regulation S–P applies to investment companies as the term is defined in Section 3 of the Investment Company Act (15 U.S.C. 80a–3), whether or not the investment company is registered with the Commission. *See* 17 CFR 248.3(r). Thus, a business development company, which is an investment company but is not required to register as such with the Commission, is subject to Regulation S–P. In this release, institutions to which Regulation S–P currently applies, or to which the proposed amendments would apply, are sometimes referred to as ''covered institutions.''

[15] 17 CFR 248.30(b). Section 216 of the FACT Act amended the FCRA by adding Section 628 (codified at 15 U.S.C. 1681w), which directed the Commission and other federal financial regulators to adopt regulations for the proper disposal of consumer information, and provides that any person who maintains or possesses consumer information or any compilation of consumer information derived from a consumer report for a business purpose must properly dispose of the information. *See Disposal of Consumer Report Information*, Exchange Act Release No. 50781, IAA Release No. 2332, ICA Release No. 26685 (Dec. 2, 2004), 69 FR 71322 (Dec. 8, 2004) (''Disposal Rule Adopting Release''). When we adopted the disposal rule, we also amended Regulation S–P to require that the policies and procedures institutions must adopt under the safeguards rule be in writing.

The disposal rule requires transfer agents registered with the Commission, as well as brokers and dealers other than notice-registered broker-dealers, investment advisers registered with the Commission, and investment companies that maintain or possess ''consumer report information'' for a business purpose, to take ''reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.''

In order to provide clarity, the Disposal Rule Adopting Release included five examples intended to provide guidance on disposal measures that would be deemed reasonable under the disposal rule. *See Disposal Rule Adopting Release* at section II.A.2.

[16] *See* Press Release, NASD, *NASD Warns Investors to Protect Online Account Information, Brokerages Also Reminded of Obligation to Protect Customer Information from New Threats* (July 28, 2005), *http://www.finra.org/PressRoom/NewsReleases/2005NewsReleases/P014775* (last visited Nov. 6, 2007). *See also In re NEXT Financial Group, Inc.*, Exchange Act Release No. 56316 (Aug. 24, 2007), *http://www.sec.gov/litigation/admin/2007/34-56316.pdf*, and Order Instituting Administrative and Cease-and-Desist Proceedings Pursuant to Sections 15(b) and 21C of the Securities Exchange Act of 1934 (Aug. 24, 2007) (alleging violations of the notice and opt out provisions of Regulation S–P and the safeguards rule in connection with recruiting registered representatives), *http://www.sec.gov/litigation/admin/2007/34-56316-o.pdf*.

[17] While some account takeovers may have been facilitated by investors failing to take adequate precautions against security threats such as

Continued

services sector also is a popular target for online targeted attacks, and ''phishing'' attacks in which fraudsters set up an Internet site designed to mimic a legitimate site and induce random Internet users to disclose personal information.[18] In other recent incidents, registered representatives of broker-dealers disposed of information and records about clients or prospective clients in accessible areas, from which journalists were able to remove them. Sensitive securities-related data also has been lost or stolen as a result of other incidents.[19]

Many firms in the securities industry are aware of these problems and have appropriate safeguards in place to address them.[20] We are concerned, however, that some firms do not regularly reevaluate and update their safeguarding programs to deal with these increasingly sophisticated methods of attack.[21] For this reason, and in light of the increase in reported security breaches and the potential for identity theft among the institutions we regulate, we believe that our previous approach, requiring safeguards that must be reasonably designed to meet the GLBA's objectives, merits revisiting.[22]

We also are concerned that while the information protected under the safeguards rule and the disposal rule includes certain personal information, it does not include other information that could be used to access investors' financial information if obtained by an unauthorized user. Finally we want to address other issues under Regulation S–P that have come to our attention, including the application of the regulation to situations in which a representative of one broker-dealer or registered investment adviser moves to another firm. Accordingly, today we are proposing amendments to the safeguards and disposal rules that are designed to address these concerns.

II. Discussion

To help prevent and address security breaches in the securities industry and thereby better protect investor information, we propose to amend Regulation S–P in four principal ways. First, we propose to require more specific standards under the safeguards rule, including standards that would apply to data security breach incidents. Second, we propose to amend the scope of the information covered by the safeguards and disposal rules and to broaden the types of institutions and persons covered by the rules. Third, we propose to require institutions subject to the safeguards and disposal rules to maintain written records of their policies and procedures and their compliance with those policies and procedures. Finally, we are taking this opportunity to propose 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.

A. Information Security and Security Breach Response Requirements

To help prevent and address security breaches at the institutions we regulate, we propose to require more specific standards for safeguarding personal information, including standards for responding to data security breaches. When we adopted Regulation S–P in 2001, the safeguards rule simply required institutions to adopt policies and procedures to address the safeguarding objectives stated in the GLBA. Following our adoption of the rule, the FTC and the Banking Agencies issued regulations with more detailed standards for safeguarding customer

---

''keylogger'' programs and ''phishing'' attacks, many online brokerage firms have successfully reduced their exposure to account takeovers by improving their authentication and monitoring procedures. The Commission has been active in this area, and has brought several enforcement cases involving defendants in foreign jurisdictions. *See, e.g.*, Litigation Release No. 20037 (Mar. 12, 2007), available at *http://www.sec.gov/litigation/litreleases/2007/lr20037.htm* (three Indian nationals charged with participating in an alleged fraudulent scheme to manipulate the prices of at least fourteen securities through the unauthorized use of other people's online brokerage accounts); and Litigation Release No. 19949 (Dec. 19, 2006), available at *http://www.sec.gov/litigation/litreleases/2006/lr19949.htm* (emergency asset freeze obtained; complaint alleged an alleged Estonia-based account intrusion scheme that targeted online brokerage accounts in the U.S. to manipulate the markets).

[18] In 2006, Symantec Corporation, a seller of information security and information management software, reported that in the first half of 2006, 84 percent of tracked phishing sites targeted the financial sector and 9 of the top 10 brands phished this period were from the financial sector. Because the financial services sector is a logical target for attackers increasingly motivated by financial gain, that sector was also the second most frequent target of Internet-based attacks (after home users). *See* Symantec, *Symantec Internet Security Threat Report, Trends for January 06–June 06*, at 9, 23 (Sept. 2006), *http://www.symantec.com/specprog/threatreport/ent-whitepaper_symantec_internet_security_threat_report_x_09_2006.en-us.pdf* (last visited Nov. 6, 2007) (''Symantec September 2006 Internet Security Threat Report''). Reportedly, employees of financial services firms ''are increasingly being invited to visit Web sites or download programs by people pretending to be colleagues or peers,'' followed by attack programs on the sites or in downloads that ''then open tunnels into the corporate network.'' More recently, although financial services-related spam reportedly ''made up 21 percent of all spam in the first six months of 2007, making it the second most common type of spam during this period,'' there was a 30-percent decline in stock market ''pump and dump'' spam ''due to a decline in spam touting penny stocks that was triggered by actions taken by the United States Securities and Exchange Commission, which limited the profitability of this type of spam by suspending trading of the stocks that are touted.'' *See Symantec, Symantec Internet Security Threat Report, Trends for January–June 07, Volume XII*, at 107 (Sept. 2007), *http://eval.symantec.com/mktginfo/enterprise/white_papers/ent-whitepaper_internet_security_threat_report_xii_09_2007.en-us.pdf* (last visited Nov. 6, 2007) (citing Commission Press Release 2007–34, *SEC Suspends Trading Of 35 Companies Touted In Spam E-mail Campaigns* (Mar. 8, 2007), available at *http://www.sec.gov/news/press/2007/2007-34.htm*).

[19] For example, in April 2005, a shipping company lost a computer backup tape containing account information for more than 200,000 broker-dealer customers. The broker-dealer voluntarily notified its affected customers, although the data was compressed and the tape was thought to have been destroyed. In December 2005, a laptop computer containing unencrypted information that included names and account numbers of 158,000 customers and the names and Social Security numbers of 68,000 adviser personnel was stolen from a registered investment adviser, and in March 2006, a laptop computer containing the names, addresses, Social Security numbers, dates of birth, and other employment-related information of as many as 196,000 retirement plan participants was stolen from a benefits plan administration subsidiary of a registered investment adviser. In both cases, the laptops were taken from vehicles by thieves who appear to have stolen them for their value as computer hardware rather than for the information contained on them. The registered investment adviser voluntarily notified the more than 200,000 clients and financial advisers whose information was compromised, while the benefits plan administrator voluntarily notified the nearly 200,000 retirement plan participants whose information was compromised, and offered to pay for a year of credit monitoring for each of them.

[20] Some institutions regulated by the Commission have already taken steps to strengthen their policies and procedures for safeguarding investors' information, such as by offering investors the use of password-generating tokens for online brokerage accounts. We also note that some firms have been sharing information about suspicious activity with one another for the purpose of combating identity theft. To the extent it might involve sharing nonpublic personal information about consumers of the firms, Regulation S–P does not prohibit such information sharing because Section 15(a)(2)(ii) of Regulation S–P permits firms to disclose nonpublic personal information to a nonaffiliated third party for the purpose of protecting against fraud without first giving consumers notice of and an opportunity to opt out of the disclosures.

[21] According to a September 2007 report from Deloitte Touche Tohmatsu, for example, 37 percent of 169 surveyed financial institutions do not have an information security strategy in place, and 33 percent of these institutions do not conduct vulnerability testing, or only do so on an ad hoc basis. *See* Deloitte Touche Tohmatsu, *2007 Global Security Survey*, at 12, 36 (Sept. 2007), *http://www.deloitte.com/dtt/cda/doc/content/dtt_gfsi_GlobalSecuritySurvey_20070901%281%29.pdf* (last visited Nov. 6, 2007).

[22] In 2004 we sought comment on whether to revise our safeguards rule to require institutions to address certain elements in designating their safeguarding policies and procedures. *See Disposal of Consumer Report Information,* Exchange Act Release No. 50361, IAA Release No. 2293, ICA Release No. 20596 (Sept. 14, 2004), 69 FR 56304 (Sept. 20, 2004) (''Disposal Rule Proposing Release''), at section II.B. At that time we decided not to revise the safeguards rule, but noted we would consider the comments we received in the event we proposed any amendment to the rule. *See Disposal Rule Adopting Release, supra* note 15, at section II.B. *See also infra* note 31.

records and information applicable to the institutions they regulate.[23] We believe these standards include necessary elements that institutions should address when adopting and implementing safeguarding policies and procedures. We have therefore looked to the other agencies' standards in developing our proposal and tailored them, where appropriate, to develop proposed standards for the institutions we regulate.

1. Revised Safeguarding Policies and Procedures

As noted above, the safeguards rule requires institutions to adopt written policies and procedures that address administrative, technical and physical safeguards to protect customer records and information. The proposed amendments would further develop this requirement by requiring each institution subject to the safeguards rule to develop, implement, and maintain a comprehensive ''information security program,'' including written policies and procedures that provide administrative, technical, and physical safeguards for protecting personal information, and for responding to unauthorized access to or use of personal information.[24] This program would have to be appropriate to the institution's size and complexity, the nature and scope of its activities, and the sensitivity of any personal information at issue.[25] Consistent with current requirements for safeguarding policies and procedures, the information security program also would have to be reasonably designed to: (i) Ensure the security and confidentiality of personal information; (ii) protect against any anticipated threats or hazards to the security or integrity of personal information; and (iii) protect against unauthorized access to or use of personal information that could result in substantial harm or inconvenience to any consumer, employee, investor or securityholder who is a natural person.[26] Although the term ''substantial harm or inconvenience'' is currently used in the safeguards rule, it is not defined. We propose to define the term to mean ''personal injury, or more than trivial financial loss, expenditure of effort or loss of time.'' [27] This definition is intended to include harms other than identity theft that may result from failure to safeguard sensitive information about an individual. For example, a hacker could use confidential information about an individual for extortion by threatening to make the information public unless the individual agrees to the hacker's demands. ''Substantial harm or inconvenience'' would *not* include ''unintentional access to personal information by an unauthorized person that results only in trivial financial loss, expenditure of effort or loss of time,'' such as if use of the information results in an institution deciding to change the individual's account number or password.[28] The rule would provide an example of what would not constitute harm or inconvenience that rises to the level of ''substantial,'' which should help clarify the scope of what would constitute ''substantial harm or inconvenience.''

The proposed amendments also would specify particular elements that a program meeting the requirements of Regulation S–P must include.[29] These elements are intended to provide firms in the securities industry with detailed standards for the policies and procedures that a well-designed information security program should include to address recent identity theft-related incidents such as firms in the securities industry losing data tapes and laptop computers and failing to dispose properly of sensitive personal information, and hackers hijacking online brokerage accounts.[30] These elements also are intended to maintain consistency with information safeguarding guidelines and rules adopted by the Banking Agencies and

[23] The Banking Agencies issued their guidelines for safeguarding customer records and information in 2001. *See Interagency Guidelines Establishing Standards for Safeguarding Customer Information and Rescission of Year 2000 Standards for Safety and Soundness,* 66 FR 8616 (Feb. 1, 2001) (''Banking Agencies'' Security Guidelines''). The FTC adopted its safeguards rule in 2002. *See Standards for Safeguarding Customer Information,* 67 FR 36484 (May 23, 2002) (''FTC Safeguards Rule''). The Banking Agencies also have jointly issued guidance on responding to incidents of unauthorized access or use of customer information. *See Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice,* 70 FR 15736 (Mar. 29, 2005) (''Banking Agencies'' Incident Response Guidance''). More recently, through the Federal Financial Institutions Examination Council (''FFIEC''), the Banking Agencies jointly issued guidance on the authentication of customers in an Internet banking environment, and the Banking Agencies and the FTC jointly issued final rules and guidelines for identity theft ''red flags'' programs to detect, prevent, and mitigate identity theft in connection with the opening of certain accounts or certain existing accounts. *See* FFIEC, *Authentication in an Internet Banking Environment* (July 27, 2006), available at *www.ffiec.gov/pdf/authentication_guidance.pdf* (''Authentication Guidance''); Banking Agencies and FTC, *Identity Theft Red Flags and Address Discrepancies under the Fair and Accurate Credit Transactions Act of 2003,* 72 FR 63718 (Nov. 9, 2007) (''Final Red Flag Rules''). *See also* Banking Agencies and FTC, *Identity Theft Red Flags and Address Discrepancies Under the Fair and Accurate Credit Transactions Act of 2003,* 71 FR 40785 (July 18, 2006) (''Proposed Red Flag Guidelines''). In March of this year, the FTC also published a brochure on data security, Protecting Personal Information: A Guide for Business (available at *http://www.ftc.gov/infosecurity/*), and the FDIC issued a *Supervisory Policy on Identity Theft,* FIL–32–2007 (Apr. 11, 2007), available at *http://www.fdic.gov/news/news/financial/2007/fil07032a.html.*

[24] As amended, Section 30 would be titled, ''Information security programs for personal information; records of compliance.''

[25] *See* proposed paragraph (a)(1) of Section 30. The term ''information security program'' would mean the administrative, technical, or physical safeguards used to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personal information. *See* proposed paragraph (d)(6) of Section 30.

[26] *See* proposed paragraph (a)(2) of Section 30. *Compare* 17 CFR 248.30(a)(1)–(3).

[27] *See* proposed paragraph (d)(12) of Section 30. ''Substantial harm or inconvenience'' would include theft, fraud, harassment, impersonation, intimidation, damaged reputation, impaired eligibility for credit, or the unauthorized use of the information identified with an individual to obtain a financial product or service, or to access, log into, effect a transaction in, or otherwise use the individual's account.

[28] *See* proposed paragraph (d)(12)(ii) of Section 30. Thus, for example the proposed definition would not encompass a firm's occasional, unintentional delivery of an individual's account statement to an incorrect address if the institution determined that the information was highly unlikely to be misused. This determination would have to be made promptly after the institution becomes aware of an incident of unauthorized access to sensitive personal information, and documented in writing. *See* proposed paragraph (a)(4)(iii) of Section 30.

[29] Many of these elements are addressed by widely accepted information security standards. *See, e.g.*, National Institute of Standards and Technology (''NIST''), Special Publication 800 series (Computer Security), for example *Generally Accepted Principals and Practices for Securing Information Technology Systems* (SP 800–14) (Sept. 1996), *Guide to Intrusion Detection and Prevention Systems* (IDPS) (SP 800–94) (Feb. 2007), and *Guide to Secure Web Services* (SP 800–95) (Aug. 2007) (all available at *http://csrc.nist.gov/publications/PubsSPs.html*), and bulletins dealing with computer security published by the NIST's Information Technology Laboratory (ITL), for example *Secure Web Servers: Protecting Web Sites That Are Accessed By The Public* (ITL January 2008) (available at *http://csrc.nist.gov/publications/PubsITLSB.html*); *Federal Information System Controls Audit Manual,* General Accounting Office, Accounting and Information Management Division, *Federal Information System Controls Audit Manual,* GAO/AIMD–12.19.6 (known as ''FISCAM'') (Jan. 1999) (available at *http://www.gao.gov/special.pubs/ai12.19.6.pdf*); International Organization for Standardization, *Code of Practice for Information Security Management* (ISO/IEC 27002:2005) (known among information security professionals as the ''British Standard,'' and formerly designated BS ISO/IEC 17799:2005 and BS 7799–1:2005) (available for purchase at *http://www.standardsdirect.org/iso17799.htm* and at *http://www.bsi-global.com/en/Shop/Publication-Detail/?pid=000000000030166440*); and Information Systems Audit and Control Association/IT Governance Institute, *Control Objectives for Information and Related Technology* (known as ''COBIT'') (last updated, and published as version 4.1, May 2007) (available at *http://www.isaca.org*).

[30] *See supra* notes 16–19 and accompanying text.

FTC.[31] In addition, these elements are consistent with policies and procedures we understand many institutions in the securities industry have already adopted. We understand that large and complex organizations generally have written policies that address information safeguarding procedures at several layers, from an organization-wide policy statement to detailed procedures that address particular controls.[32]

Institutions subject to the rule would be required to:

(i) Designate in writing an employee or employees to coordinate the information security program; [33]

(ii) Identify in writing reasonably foreseeable security risks that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of personal information or personal information systems; [34]

(iii) Design and document in writing and implement information safeguards to control the identified risks; [35]

(iv) Regularly test or otherwise monitor and document in writing the effectiveness of the safeguards' key controls, systems, and procedures, including the effectiveness of access controls on personal information systems, controls to detect, prevent and respond to attacks, or intrusions by unauthorized persons, and employee training and supervision; [36]

(v) Train staff to implement the information security program; [37]

(vi) Oversee service providers by taking reasonable steps to select and retain service providers capable of maintaining appropriate safeguards for the personal information at issue, and require service providers by contract to implement and maintain appropriate safeguards (and document such oversight in writing); [38] and

(vii) Evaluate and adjust their information security programs to reflect the results of the testing and monitoring, relevant technology changes, material changes to operations or business arrangements, and any other circumstances that the institution knows or reasonably believes may have a material impact on the program.[39]

The term ''service provider'' would mean 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.[40] We understand that in large financial complexes, a particular affiliate may be responsible for providing a particular service for all affiliates in the complex. In that circumstance, each financial institution subject to Regulation S–P would be responsible for taking reasonable steps to ensure that the service provider is capable of maintaining appropriate safeguards and of overseeing the service provider's implementation, maintenance, evaluation, and modifications of appropriate safeguards for the institution's personal information. Under the proposed amendments, we anticipate that a covered institution's reasonable steps to evaluate the information safeguards of service providers could include the use of a third-party review of those safeguards such as a Statement of Auditing Standards No. 70 (''SAS 70'') report, a SysTrust report, or a WebTrust report.[41]

We request comment on the proposed specific standards for safeguarding personal information.

- Would these standards provide sufficient direction to institutions? Are there particular standards that should be more or less prescriptive? For example, should institutions be required to designate an employee or employees to coordinate the information security program by name, or should institutions be permitted to make these designations by position or office?
- Would additional standards be appropriate or are certain standards unnecessary? Should the proposed standards be modified to more closely or less closely resemble standards prescribed by the Banking Agencies or the FTC? For the securities industry, are there any other standards that a well-designed information security program should address? Are there any other standards that would provide more flexibility to covered institutions?
- We also invite comment on the proposed requirement that entities assess the sufficiency of safeguards in place, to control reasonably foreseeable risks. Should the rules include more detailed standards and specifications for access controls? Should the requirement specify factors such as those identified in the Banking Agencies' guidance regarding authentication in an Internet banking environment or include policies and procedures such as those in the Banking Agencies and the FTC's proposed or final ''red flag'' requirements? [42] For example, should we require that covered institutions implement multifactor authentication, layered security, or other controls for high-risk transactions involving access to customer information or the movement of funds to third parties? Should we require that covered institutions include in their information security programs ''red flag'' elements

[31] *See* Banking Agencies' Security Guidelines and FTC Safeguards Rule, *supra* note 23. As noted above, we sought comment on whether to revise our safeguards rule in 2004. *See supra* note 22. At that time, several commenters noted that Rule 206(4)–7 under the Investment Advisers Act (17 CFR 275.206(4)–7) and Rule 38a–1 under the Investment Company Act (17 CFR 270.38a–1) require registered investment advisers and registered investment companies to have written policies and procedures reasonably designed to prevent violation of the federal securities laws, including safeguards for the protection of customer records and information under Regulation S–P. These rules also require registered investment advisers and funds to review, no less frequently than annually, the adequacy of these policies and procedures. *See* Comment Letter of the Investment Counsel Association of America (Oct. 20, 2004), at p. 3; Comment Letter of the Investment Company Institute (Oct. 20, 2004) at p. 2. Each of these letters is available at *http://www.sec.gov/comments/s73304.shtml.* We do not intend for the proposed amendments to alter or conflict with these requirements.

[32] *See Disposal Rule Proposing Release, supra* note 22, at 69 FR 56308 & n.29.

[33] *See* proposed paragraph (a)(3)(i) of Section 30. Of course, the employee or employees designated to coordinate an institution's information security program would need to have sufficient authority and access to the institution's managers, officers and directors to effectively implement the program and modify it as necessary.

[34] *See* proposed paragraph (a)(3)(ii) of Section 30. The term ''personal information system'' would mean any method used to access, collect, store, use, transmit, protect or dispose of personal information. *See* proposed paragraph (d)(9) of Section 30.

[35] *See* proposed paragraph (a)(3)(iii) of Section 30.

[36] *See* proposed paragraph (a)(3)(iv) of Section 30.

[37] *See* proposed paragraph (a)(3)(v) of Section 30.

[38] *See* proposed paragraph (a)(3)(vi) of Section 30.

[39] *See* proposed paragraph (a)(3)(vii) of Section 30. This requirement is similar to the requirement in the Banking Agencies' Security Guidelines that institutions covered by those guidelines monitor, evaluate, and adjust, as appropriate, their information security program in light of any relevant changes in technology, the sensitivity of their customer information, internal or external threats to information, and their own changing business arrangements, such as mergers and acquisitions, alliances and joint ventures, outsourcing arrangements, and changes to customer information systems. *See supra* note 23, Banking Agencies' Security Guidelines, 66 FR at 8634, 8635–36, 8637, 8639, 8641. The ''material impact'' standard in proposed paragraph (a)(3)(iii) is intended to require adjustment of a covered institution's information security program only when a reasonable coordinator of the program would consider adjusting the program important in light of changing circumstances.

[40] *See* proposed paragraph (d)(11) of Section 30.

[41] *See* Codification of Accounting Standards and Procedures, Statement on Auditing Standards No. 70, Reports on Processing of Transactions by Service Organizations (American Inst. of Certified Public Accountants). *See also* description and comparison of these reports at *http://infotech.aicpa.org/Resources/System+Security+and+Reliability/System+Reliability/Principles+of+a+Reliable+System/SAS+No+70+SysTrust+and+WebTrust+A+Comparison.htm.*

[42] *See* Authentication Guidance, Proposed Red Flag Guidance, and Final Red Flag Rules, *supra* note 23. The Authentication Guidance has been credited with helping to curtail online banking fraud, but has been characterized as not adequately addressing authentication in the context of telephone banking. *See* Daniel Wolfe, *How New Authentication Systems are Altering Fraud Picture,* Amer. Banker (Dec. 26, 2007).

that would be relevant to detecting, preventing and mitigating identity theft in connection with the opening of accounts or existing accounts, or in connection with particular types of accounts associated with a reasonably foreseeable risk of identity theft? Should we require that covered institutions adopt policies and procedures for evaluating changes of address followed closely by an account change or transaction, or for processing address discrepancy notices from consumer reporting agencies? If the rule were to include more detailed standards and specifications for access controls, how should these apply to business conducted by telephone?

• Commenters are invited to discuss the proposed definition of ''substantial harm or inconvenience.'' Are there circumstances that commenters believe would create substantial harm or inconvenience to individuals that would not meet the proposed definition? If so, how should the definition be revised to address these circumstances?

• Commenters are invited to discuss the proposed requirements for written documentation of compliance with the proposed safeguarding provisions.

• Commenters are invited to discuss the proposed definition of ''service provider.'' They also are invited to discuss whether, if the proposed amendments are adopted, they should include or be accompanied by guidance on the use of outside evaluations of third-party service providers. For example, should the Commission provide guidance similar to that provided by the FFIEC on the appropriate use of SAS 70 reports in evaluating the information safeguards of service providers? [43]

2. Data Security Breach Response

Because of the potential for harm or inconvenience to individuals when a data security breach occurs, we are proposing that information security programs include procedures for responding to incidents of unauthorized access to or use of personal information. These procedures would include notice to affected individuals if misuse of sensitive personal information has occurred or is reasonably possible. The procedures would also include notice to the Commission (or for certain broker-dealers, their designated examining authority [44]) 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. The proposed rules that would require prompt notice of information security breach incidents to individuals, as well as the Commission or designated examining authorities, are intended to facilitate swift and appropriate action to minimize the impact of the security breach.

The data security breach response provisions of the proposed amendments include elements intended to provide firms in the securities industry with detailed standards for responding to a breach so as to protect against unauthorized use of compromised data. The proposed standards would specify procedures a covered institution's information security program would need to include. These procedures would be required to be written to provide clarity for firm personnel and to facilitate Commission and SRO examination and inspection. The proposed standards are intended to ensure that covered institutions adopt plans for responding to an information security breach incident so as to minimize the risk of identity theft or other significant investor harm or inconvenience from the incident. These proposed procedures also are intended to be consistent with security breach notification guidelines adopted by the Banking Agencies.[45]

Under the proposed amendments, institutions subject to the rule would be required to have written procedures to:

(i) Assess any incident involving unauthorized access or use, and identify in writing what personal information systems and what types of personal information may have been compromised; [46]

(ii) Take steps to contain and control the incident to prevent further unauthorized access or use and document all such steps taken in writing; [47]

(iii) Promptly conduct a reasonable investigation and determine in writing the likelihood that the information has been or will be misused after the institution becomes aware of any unauthorized access to sensitive personal information; [48] and

(iv) Notify individuals with whom the information is identified as soon as possible (and document the provision of such notification in writing) if the institution determines that misuse of the information has occurred or is reasonably possible.[49]

We propose to define the term, ''sensitive personal information,'' to mean ''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 name, telephone number, street address, e-mail address, or online user name, in combination with any one

[43] The FFIEC provided the following guidance on the use of SAS 70 reports in the oversight of third-party service providers (''TSPs'') by financial institutions regulated by FFIEC member agencies:

Financial institutions should ensure TSPs implement and maintain controls sufficient to appropriately mitigate risk. In higher-risk relationships the institution by contract may prescribe minimum control and reporting standards, obtain the right to require changes to standards as external and internal environments change, and obtain access to the TSP for institution or independent third-party evaluations of the TSP's performance against the standard. In lower risk relationships the institution may prescribe the use of standardized reports, such as trust services reports or a Statement of Auditing Standards 70 (SAS 70) report.

* * * * *

Financial institutions should carefully and critically evaluate whether a SAS 70 report adequately supports their oversight responsibilities. The report may not provide a thorough test of security controls and security monitoring unless requested by the TSP. It may not address the effectiveness of the security process in continually mitigating changing risks. Additionally, the SAS 70 report may not address whether the TSP is meeting the institution's specific risk mitigation requirements. Therefore, the contracting oversight exercised by financial institutions may require additional tests, evaluations, and reports to appropriately oversee the security program of the service provider.

FFIEC, *FFIEC IT Examination Handbook, Information Security Booklet—July 2006,* at 77, 78 (available at *http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf*).

[44] A broker-dealer's designated examining authority is the self-regulatory organization (''SRO'') of which the broker-dealer is a member, or, if the broker-dealer is a member of more than one SRO, the SRO designated by the Commission pursuant to 17 CFR 240.17d–1 as responsible for examination of the member for compliance with applicable financial responsibility rules (including the Commission's customer account protection rules at 17 CFR 240.15c3–3).

[45] *See* Banking Agencies' Incident Response Guidance, *supra* note 23.

[46] *See* proposed paragraph (a)(4)(i) of Section 30.

[47] *See* proposed paragraph (a)(4)(ii) of Section 30.

[48] *See* proposed paragraph (a)(4)(iii) of Section 30.

[49] *See* proposed paragraph (a)(4)(iv) of Section 30. Notification could be delayed, however, if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and requests in writing a delay in notification. We propose to require notification of individuals only if misuse of the compromised information has occurred or is reasonably possible to avoid requiring notification in circumstances in which there is no significant risk of substantial harm or inconvenience. If covered institutions were required to notify individuals of every instance of unauthorized access or use, such as if an employee accidentally opened and quickly closed an electronic account record, individuals could receive an excessive number of data breach notifications and become desensitized to incidents that pose a real risk of identity theft.

of the individual's account number, credit or debit card number, driver's license number, credit card expiration date or security code, mother's maiden name, password, personal identification number, biometric authentication record, or other authenticating information.[50] This definition is intended to cover the types of information that would be most useful to an identity thief, and to which unauthorized access would create a reasonable possibility of substantial harm or inconvenience to an affected individual.

The amendments also would require an institution to provide notice to the Commission as soon as possible after the institution becomes aware of any incident of unauthorized access to or use of personal information in which there is a significant risk that an individual identified with the information might suffer substantial harm or inconvenience, or in which an unauthorized person has intentionally obtained access to or used sensitive personal information.[51] This requirement would allow Commission and SRO investigators or examiners to review the notices to determine if an immediate investigative or examination response would be appropriate. In this regard, it is crucial that institutions respond promptly to any follow-up requests for records or information from our staff or the staff of the designated examining authority.[52] Under the proposed amendments, a prompt response in accordance with existing Commission guidance on the timely production of records would be particularly important in circumstances involving ongoing misuse of sensitive personal information.

The regulatory notification requirement in the Banking Agencies' guidance requires a report to the appropriate regulator as soon as possible after the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information.[53] Our proposed notice requirement differs from the Banking Agencies' approach in that it would require notice to the Commission (or a designated examining authority) when an incident of unauthorized access to or use of personal information poses a significant risk that an individual identified with the information might suffer substantial harm or inconvenience, or in which an unauthorized person has intentionally obtained access to or used sensitive personal information. The proposed notice requirement is intended to avoid notice to the Commission in every case of unauthorized access, and to focus scrutiny on information security breaches that present a greater potential likelihood for harm. We believe that this approach would help conserve institutions', as well as the Commission's, administrative resources by allowing minor incidents to be addressed in a way that is commensurate with the risk they present. The information to be included in the notice would allow the Commission or a broker-dealer's designated examining authority to evaluate whether any legal action against a would-be identity thief or other action is warranted in light of the circumstances. A broker-dealer, other than a notice-registered broker dealer, would be required to notify the appropriate designated examining authority on proposed Form SP–30. An investment company or registered investment adviser or transfer agent would be required to notify the Commission on proposed Form SP–30.[54]

Proposed Form SP–30 would require the institution to disclose information that the Commission (or the designated examining authority) needs to understand the nature of the unauthorized access or misuse of personal information and the institution's intended response to the incident.[55] Accordingly, in addition to identifying and contact information for the covered institution, the form would request a description of the incident, when it occurred and what offices or parts of the registrant's business were affected. The form also would require disclosure of any third-party service providers that were involved, the type of services provided and, if the service provider is an affiliate, the nature of the affiliation. This information would help examiners to assess the information security policies and procedures of the service provider. In addition, the form would require a description of any customer account losses.

Under the proposed amendments, if a covered institution determined that an unauthorized person had obtained access to or used sensitive personal information, and that misuse of the information had occurred or was reasonably possible, the institution also would be required to provide notification, in a clear and conspicuous manner, to each individual identified with the information.[56] The proposed requirements for notices to individuals are intended to give investors information that would help them protect themselves against identity theft. They also are intended to be consistent with similar requirements in the Banking Agencies' Incident Response Guidance.[57]

The notices to affected individuals that would be required by the proposed amendments would have to:

(i) Describe the incident and the type of information that was compromised, and what was done to protect the individual's information from further unauthorized access or use;[58]

(ii) Include a toll-free telephone number or other contact information for further information and assistance from the institution;[59]

(iii) Recommend that the individual review account statements and immediately report any suspicious activity to the institution;[60] and

(iv) Include information about FTC guidance regarding the steps an individual can take to protect against identity theft, a statement encouraging the individual to report any incidents of identity theft to the FTC, and the FTC's Web site address and toll-free telephone number for obtaining identity theft guidance and reporting suspected incidents of identity theft.[61]

[50] *See* proposed paragraph (d)(10) of Section 30.

[51] *See* proposed paragraph (a)(4)(v) of Section 30.

[52] *See generally* 15 U.S.C. 21(a) (investigative requests); 17 CFR 240.17a 4(j) (examinations of broker-dealers); 17 CFR 275.204–2(g) (examinations of investment advisers).

[53] *See* Banking Agencies' Incident Response Guidance, *supra* note 23, at 70 FR 15740–15741 (concluding that the Banking Agencies' standard for notification to regulators should provide an early warning to allow an institution's regulator to assess the effectiveness of an institution's response plan, and, where appropriate, to direct that notice be given to customers if the institution has not already done so).

[54] We anticipate that this form could be downloaded from our Web site and would be required to be filed electronically with the Registrations Branch in the Office of Compliance Inspections and Examinations. While broker-dealers generally would file the form with their designated examining authority rather than the Commission, investment advisers that are dually registered with the Commission as broker-dealers also would file with the Commission and indicate their dual-registrant status on the form.

[55] *See* proposed Form SP–30. Information submitted to the Commission on the form would be accorded confidential treatment to the extent permitted by law. *See, e.g.*, 17 CFR 200.83. We realize that the full amount of losses may not be known at the time an information security breach is discovered, but we would expect covered institutions to make a good faith effort to complete the proposed form to the extent possible.

[56] *See* proposed paragraph (a)(5) of Section 30.

[57] *See* Banking Agencies' Incident Response Guidance, *supra* note 23.

[58] *See* proposed paragraphs (a)(5)(i) and (a)(5)(ii) of Section 30.

[59] *See* proposed paragraph (a)(5)(iii) of Section 30.

[60] *See* proposed paragraphs (a)(5)(iv) and (a)(5)(v) of Section 30.

[61] *See* proposed paragraph (a)(5)(vi) of Section 30.

We request comment on the proposed specific standards relating to incidents of unauthorized access to or misuse of personal information.

• Commenters are invited to discuss the proposed requirements for procedures for responding to incidents of unauthorized access to or use of personal information. Are there any particular steps that may not be necessary, or not necessary in all situations? Are there any other steps that could be taken in response to a security breach that also should be required in some or all situations?

• We request comment on the proposed provisions regarding procedures for notifying the Commission (or a broker-dealer's designated examining authority) of incidents in which an individual identified with compromised information has suffered substantial harm or inconvenience, or an unauthorized person has intentionally obtained access to or used sensitive personal information.

• For example, should firms be required to provide notice only if the information compromised in an incident is identified with a certain number of individuals? Should the rule include a numerical or other threshold for when notice to the Commission (or to a broker-dealer's designated examining authority) is required? If so, how would a threshold work for smaller institutions that may be far more likely than larger institutions to meet the threshold? Will the proposed standard provide a sufficient early warning to the Commission, or should the Commission broaden the circumstances under which notices would be required to be provided to the Commission (or to a broker-dealer's designated examining authority), such as the standard adopted by the Banking Agencies? Commenters should explain their views.

• Is the proposed definition of ''sensitive personal information'' sufficient? Are there particular types of information that should or should not be included?

• We request comment on proposed Form SP–30. Is the form easy to understand and use? For example, is the form clear, or would additional guidance, such as instructions or further explanation of particular questions or terms be helpful? Would it be easier or more cost-effective for firms if the rule specified the information they are required to provide rather than provide a form? Would the form be more useful if it were in a tabular format? Commenters should be specific regarding changes they believe should be made to the content or format of the proposed form.

• Similarly, we invite comment on the proposed provisions regarding procedures for notifying individuals of incidents of unauthorized use or access if an institution determines that an unauthorized person has obtained access to or used the information and that misuse of sensitive personal information has occurred or is reasonably possible. Is the information in the proposed notice to individuals appropriate? Is there additional information that institutions should include, or information, proposed to be included, that should be eliminated? Is the proposed threshold for notice appropriate? If not, are there alternative thresholds for notice to individuals that would be more appropriate? If so, commenters should explain their views.

• Commenters are invited to discuss the proposed requirements for written documentation of compliance with the proposed incident response provisions.

B. Scope of the Safeguards and Disposal Rules

1. Information Covered by the Safeguards and Disposal Rules

The Commission adopted the safeguards and disposal rules at different times under different statutes—respectively, the GLBA and the FACT Act—that differ in the scope of information they cover. As noted above, Regulation S–P implements the GLBA privacy provisions governing requirements for notice and opt out before an institution can share certain information with nonaffiliates and for safeguarding information. The regulation's notice and opt out provisions limit institutions from sharing ''nonpublic personal information'' about consumers and customers as defined in the GLBA and in Regulation S–P, with nonaffiliated third parties.[62] As required under the GLBA, the safeguards rule requires covered institutions to maintain written policies and procedures to protect ''customer records and information,''[63] which is not defined in the GLBA or in Regulation S–P. The disposal rule requires institutions to properly dispose of ''consumer report information,'' a third term, which Regulation S–P defines consistent with the FACT Act provisions.[64] Each of these terms includes a different set of information, although the terms include some of the same information.[65] Each term also does *not* include some information that, if obtained by an unauthorized user, could permit access to personal financial information about an institution's customers. We preliminarily believe that in order to provide better protection against the unauthorized disclosure of this personal financial information, the scope of information protected by both the safeguards rule and the disposal rule should be broader. Broadening the scope of information covered by the safeguards and disposal rules would more appropriately implement Section 525 of the GLBA. Section 525 directs the Commission to revise its regulations as necessary to ensure that covered institutions have policies, procedures, and controls in place to prevent the unauthorized disclosure of ''customer financial information.'' Section 521 of Title V of the GLBA prohibits persons from obtaining or requesting a person to obtain, customer information by making false or fraudulent statements to an officer, employee, agent, or customer of a financial institution.[66] In furtherance of these prohibitions, the GLBA directs the Commission and the other federal financial regulators to review their regulations and to revise them as necessary to ensure that financial institutions have policies, procedures and controls in place to prevent the unauthorized disclosure of ''customer financial information'' and to deter and detect the activity described in Section 521.[67] Applying both the safeguards and disposal rules to a consistent set of information also could reduce any burden that may have been created by the application of the safeguards and disposal rules to different information.[68]

[62] *See* 15 U.S.C. 6802(a), (b). ''Nonpublic personal information'' is generally defined in the GLBA and Regulation S–P as encompassing personally identifiable financial information, as well as any list, description, or other grouping of consumers (and publicly available information pertaining to them) derived using any personally identifiable financial information that is not publicly available, subject to certain exceptions. *See* 15 U.S.C. 6809(4); 17 CFR 248.3(t) and 248.3(u). *See supra* note 12 for a discussion of the notice and opt out provisions.

[63] *See* 17 CFR 248.30; 15 U.S.C. 6801(b)(1).

[64] 17 CFR 248.30(b)(2). Section 628(a)(1) of the FCRA directed the Commission to adopt rules requiring the proper disposal of ''consumer information, or any compilation of consumer information, derived from consumer reports for a business purpose.'' 15 U.S.C. 1681w(a)(1). Regulation S–P uses the term ''consumer report information'' and defines it to mean a record in any form about an individual ''that is a consumer report or is derived from a consumer report.'' 17 CFR 248.30(b)(1)(ii). ''Consumer report'' has the same meaning as in Section 603(d) of the Fair Credit Reporting Act (15 U.S.C. 1681(d)). 17 CFR 248.30(b)(1)(i).

[65] *See* Disposal Rule Adopting Release, *supra* note 15, at 69 FR 71323 n.13.

[66] *See* 15 U.S.C. 6821(a), (b).

[67] *See* 15 U.S.C. 6825.

[68] *See* David Annecharico, Note, *Online Transactions: Squaring the Gramm-Leach-Bliley Act*

Continued

Accordingly, we propose to amend the safeguards and disposal rules so that both protect ''personal information,'' and to define that term to encompass any record containing either ''nonpublic personal information'' or ''consumer report information.'' [69] As noted above, each of these terms is defined in Regulation S–P.[70] The term ''consumer report information'' would continue to mean any record about an individual, whether in paper, electronic or other form, that is a consumer report or is derived from a consumer report, as well as a compilation of such records, but not including information that does not identify individuals, such as aggregate information or blind data.[71] The proposed amendments would leave the meaning of the term ''consumer report'' unchanged from the definition set forth in Section 603(d) of the FCRA.[72] Section 603(d) defines ''consumer report'' in general as encompassing communications of information by a consumer reporting agency bearing on a consumer's creditworthiness, credit standing, reputation or particular other factors used in connection with establishing the consumer's eligibility for credit or insurance, or for employment purposes or other authorized purposes, subject to certain exclusions.[73]

In addition to nonpublic personal information and consumer report information, ''personal information'' also would include information identified with any consumer, or with any employee, investor, or securityholder who is a natural person,[74] in paper, electronic or other form, that is handled by the institution or maintained on the institution's behalf.[75] Thus, for example, the definition would include records of employee user names and passwords maintained by a brokerage firm, and records about securityholders maintained by a transfer agent. We believe safeguarding employee user names and passwords promotes information security because unauthorized access to this information could facilitate unauthorized access to a firm's network and its clients' personal information.[76] Safeguarding information about investors and securityholders, such as maintained by registered transfer agents, is necessary to protect investors who may, directly or indirectly, do business with the Commission's regulated entities even though they may not be ''consumers'' or ''customers'' of those entities as those terms are defined for purposes of Regulation S–P.[77] We also propose to make a conforming change to the definition of ''personally identifiable financial information'' by including within the definition information that is handled or maintained by a covered institution or on its behalf, and that is identified with any consumer, or with any employee, investor, or securityholder who is a natural person.[78] We preliminarily believe that this change would be appropriate in the public interest and for the protection of investors because it would help protect information identified with an investor who may not be a ''consumer'' or ''customer'' of a covered institution.

To better protect investors'' and securityholders' information from unauthorized disclosure, the proposed amendments would apply the safeguards and disposal rules to nonpublic personal information or consumer report information that is identified with any individual consumer, employee, investor or securityholder and handled or maintained by or on behalf of the institution. The proposal to include personal information and consumer report information about employees of covered institutions is intended to reduce the risk that a would-be identity thief could access investor information by impersonating an employee or employing ''social engineering'' techniques or bribery.

Including consumer report information within the definition of ''personal information'' (to which the safeguards rule would apply) would be consistent with the congressional intent behind making consumer report information subject to the disposal requirements set forth in the FACT Act.[79] Furthermore, the proposed scope of protection appears to be consistent with the practices of many covered institutions that currently protect employee information, consumer report information, and nonpublic personal information about consumers and customers in the same manner.[80]

We invite comment on the proposed definition of ''personal information.''

- Should the safeguards rule extend to consumer report information that is not nonpublic personal information?
- Should the disposal rule extend to nonpublic personal information that is not consumer report information?
- To what extent do institutions currently take the same measures in disposing of consumer report information, customer records and information, nonpublic personal information about consumers and customers, and information other than consumer report information that is identified with employees, investors, or securityholders who are not consumers or customers? To the extent that measures are different, what is the basis for those differences?
- Is the proposed definition of ''personal information,'' which includes all records containing either consumer report information or nonpublic personal information, broad enough to encompass the information that needs to be protected? If not, how should we expand the definition? Are there any aspects of the proposed definition that, in the context of the information security requirements discussed below, may be over-inclusive with regard to particular types of entities? If so, how should we tailor the definition?
- The proposed definition of ''personal information'' encompasses

Privacy Provisions With the FTC Fair Information Practice Principles, 6 N.C. Banking Inst. 637, 662 (2002), available at *http://www.unc.edu/ncbank/Articles%20and%20Notes%20PDFs/Volume%206/DavidAnnecharico%5Bpp637-664%5D.pdf* (''To require financial institutions to treat the security of consumer information on par with customer information may be cost effective and efficient. It could merely mean storing consumer information within the already mandated secure storage systems that are being used to store customer information.'').

[69] Proposed paragraph (d)(8) of Section 30.

[70] *See* 17 CFR 248.3(t)(1) (definition of ''nonpublic personal information''); 17 CFR 248.30(b)(ii) (definition of ''consumer report information'').

[71] *See* proposed paragraph (c)(4) of Section 30 and current paragraph (b)(ii) of Section 30 (definition governing current disposal requirements).

[72] *See* proposed paragraph (d)(3) of Section 30.

[73] *See* 15 U.S.C. 1681a(d).

[74] This element of the definition would exclude information identified only with persons other than natural persons, such as corporations. The GLBA limits the protections provided under subtitle A of the privacy provisions to ''consumers,'' who are *individuals* who obtain from a financial institution financial products or services to be used for personal, family or household purposes. 15 U.S.C. 6809(9). The FACT Act defines a ''consumer'' to mean an individual. 15 U.S.C. 1681a(c).

[75] *See* proposed paragraph (d)(8) of Section 30.

[76] *See supra* note 17 and accompanying text.

[77] As discussed *supra* at note 7, Regulation S–P defines the terms ''consumer'' and ''customer'' at 17 CFR 248.3(g) and 248.3(j), respectively.

[78] *See* proposed new paragraph (u)(1)(iv) of Section 3. The proposed amendments also would include technical, conforming changes to references to Section 30 in Sections 1(b) and 2(b) of Regulation S–P.

[79] The disposal rule was intended to reduce the risk of fraud or related crimes, including identity theft, by ensuring that records containing sensitive financial or personal information are appropriately redacted or destroyed before being discarded. *See* 108 Cong. Rec. S13,889 (Nov. 4, 2003) (statement of Sen. Nelson).

[80] Based on our staff's informal discussions with industry representatives about Regulation S–P issues, as well as the estimated costs and benefits of the proposed amendments we believe that many covered institutions currently protect both kinds of information in the same way out of prudence and for reasons of operational efficiency. *See infra* section V.B.

information identified with any consumer, or with any employee, investor, or securityholder who is a natural person. Are there any other persons whose information should be protected under the safeguards rule, or should the safeguards rule cover only information identified with individuals who are customers of a financial institution?

• Should the proposed definition of ''personal information'' be expanded to include information identified with non-natural persons, such as corporate clients? Commenters should explain their views.

2. Institutions Covered by the Safeguards Rule

As discussed above, the safeguards rule currently applies to brokers, dealers, registered investment advisers, and investment companies. The disposal rule currently applies to those entities as well as to registered transfer agents. We propose to extend the safeguards rule to apply to registered transfer agents.[81] These institutions, like those currently subject to both the safeguards and disposal rules, may maintain personal information such as Social Security numbers, account numbers, passwords, account balances, and records of securities transactions and positions. Unauthorized access to or misuse of such information could result in substantial harm and inconvenience to the individuals identified with the information. The proposed amendments thus would require that covered institutions that may receive personal information in the course of effecting, processing or otherwise supporting securities transactions must protect that information by maintaining appropriate safeguards in addition to taking measures to properly dispose of the information.[82] Registered transfer agents may maintain sensitive personal information about investors, the unauthorized access to or use of which could cause investors substantial inconvenience or harm. Therefore, we preliminarily believe that extending the safeguards rule to registered transfer agents would be appropriate in the public interest and for the protection of investors.[83]

The proposed amendments also would limit the scope of broker-dealers covered by the safeguards rule to brokers or dealers other than those registered by notice with the Commission under Section 15(b)(11) of the Exchange Act.[84] Notice-registered broker-dealers must comply with the privacy rules, including rules requiring the safeguarding of customer records and information, adopted by the CFTC.[85] Excluding notice-registered broker-dealers from the scope of the Commission's safeguards rule would clarify that both sets of rules do not apply to notice-registered broker-dealers, and that the CFTC would have primary responsibility for oversight of those broker-dealers in this area.

We seek comment on the proposed scope of the safeguards rule.

• Should registered transfer agents be subject to the safeguards rule? To what extent are registered transfer agents expected to possess, or lack, the type of information that could be used to commit identity theft or otherwise cause individuals substantial harm or inconvenience?[86] Are there special issues that registered transfer agents might have in implementing or meeting the requirements of the safeguards rule?

• Should the Commission propose to extend the safeguards and disposal rules to self-regulatory organizations or other types of institutions in the securities industry? If so, which ones?

• Should notice-registered broker-dealers be excluded from the scope of the proposed amended safeguards rule? If not, why not?

3. Persons Covered by the Disposal Rule

As noted above, the disposal rule currently applies to broker-dealers, investment companies, registered investment advisers and registered transfer agents. We propose to extend the disposal rule to apply to natural persons who are associated persons of a broker or dealer, supervised persons of a registered investment adviser, and associated persons of a registered transfer agent.[87] As noted above, we have become concerned that some of these persons, who may work in branches far from the registered entity's main office, may not dispose of sensitive personal financial information consistent with the registered entity's disposal policies. The proposal is intended to make persons associated with a covered institution directly responsible for properly disposing of personal information consistent with the institution's policies.

• We request comment on the proposed extension of the scope of the disposal rule to apply to natural persons who are associated with broker-dealers, supervised persons of registered investment advisers, or who are associated persons of registered transfer agents.

• Are there alternative ways of helping to ensure that these persons would follow the covered institution's disposal policies and properly dispose of personal information?

[81] The term ''transfer agent'' would be defined by proposed paragraph (d)(14) of Section 30 to have the same meaning as in Section 3(a)(25) of the Exchange Act (15 U.S.C. 78c(a)(25)).

As discussed below, we also propose to extend the disposal rule to associated persons of broker-dealers, supervised persons of registered investment advisers, and associated persons of registered transfer agents.

[82] The proposed definition of ''personal information'' would include information about individual investors maintained by registered transfer agents even though transfer agents typically do not have consumers or customers for purposes of Regulation S–P because their clients generally are not individuals, but are the companies in which investors, including individuals, hold shares.

[83] Under Section 17A of the Exchange Act (15 U.S.C. 78q–1) the Commission has authority to prescribe rules and regulations for transfer agents as necessary or appropriate in the public interest, for the protection of investors, or otherwise in furtherance of the purposes of Title I of the Exchange Act.

[84] Proposed paragraph (a)(1) of Section 30. *See* 15 U.S.C. 78*o*(b)(11). The Commodity Futures Modernization Act of 2000 established a system of notice registration under which trading facilities and intermediaries that are already registered with either the Commission or the CFTC may register with the other agency on an expedited basis for the limited purpose of trading security futures products. Under the substituted compliance provision in Section 2(b) of Regulation S–P (17 CFR 248.2(b)), CFTC-regulated futures commission merchants and introducing brokers that are registered by notice with the Commission and in compliance with the financial privacy rules of the CFTC are deemed to be in compliance with Regulation S–P, except with respect to Regulation S–P's disposal rule (currently 17 CFR 248.30(b)). Notice-registered broker-dealers are already excluded from the scope of the disposal rule.

[85] *See* 17 CFR 160.30.

[86] Such information could include address and account information used to disseminate shareholder communications and dividend and interest payments, as well as information collected pursuant to Rule 17Ad–17 under the Exchange Act (17 CFR 240.17Ad–17), which requires transfer agents registered with the Commission to use taxpayer identification numbers or names to search databases for addresses of lost securityholders.

[87] *See* proposed paragraph (b)(1) of Section 30. The term ''associated person of a broker or dealer'' would be defined by proposed paragraph (d)(1) of Section 30 to have the same meaning as in Section 3(a)(18) of the Exchange Act (15 U.S.C. 78c(a)(18)). The term ''supervised person of an investment adviser'' would be defined by proposed paragraph (d)(13) of Section 30 to have the same meaning as in Section 202(a)(25) of the Investment Advisers Act of (15 U.S.C. 80b–2(a)(25)). We are proposing to include ''supervised'' persons of an investment adviser, rather than ''associated'' persons in order to include all employees, including clerical employees, of an investment adviser who may be responsible for disposing of personal information. *See* 15 U.S.C. 80b–2(a)(17) (defining term ''person associated with an investment adviser'' not to include associated persons whose functions are clerical or ministerial). This approach is intended to cover the same range of employees as investment advisers, broker-dealers, and registered transfer agents. The term ''associated person of a transfer agent'' would be defined by proposed paragraph (d)(2) of Section 30 to have the same meaning as in Section 3(a)(49) of the Exchange Act (15 U.S.C. 78c(a)(49).

An additional proposed extension to the scope of the disposal rule is discussed below. *See infra* section II.B.

C. Records of Compliance

We further propose to amend Regulation S–P to require institutions subject to the safeguards and disposal rules to make and preserve written records of their safeguards and disposal policies and procedures. We also propose to require that institutions document that they have complied with the elements required to develop, maintain and implement these policies and procedures for protecting and disposing of personal information, including procedures relating to incidents of unauthorized access to or misuse of personal information. These records would help institutions assess their policies and procedures internally, and help examiners to monitor compliance with the requirements of the amended rules. The periods of time for which the records would have to be preserved would vary by institution, because the requirements would be consistent with existing recordkeeping rules, beginning with when the records were made, and, for records of written policies and procedures, after any change in the policies or procedures they document.[88] Broker-dealers would have to preserve the records for a period of not less than three years, the first two years in an easily accessible place. Registered transfer agents would have to preserve the records for a period of not less than two years, the first year in an easily accessible place. Investment companies would have to preserve the records for a period not less than six years, the first two years in an easily accessible place. Registered investment advisers would have to preserve the records for five years, the first two years in an appropriate office of the investment adviser. We believe that these proposed recordkeeping provisions, while varying among covered institutions, would all result in the maintenance of the proposed records for sufficiently long periods of time and in locations in which they would be useful to examiners. Moreover, we do not believe that shorter or longer maintenance periods would be warranted by any difference between the proposed records and other records that covered institutions currently must maintain for these lengths of time. We also believe that conforming the proposed retention periods to existing requirements would allow covered institutions to minimize their compliance costs by integrating the proposed requirements into their existing recordkeeping systems.[89]

We request comment on the proposed requirements for making and retaining records.

- Are the proposed periods of time for preserving the records appropriate, or should certain records be preserved for different periods of time?
- Would the costs associated with preserving records for periods of time consistent with covered institutions' other recordkeeping requirements be less than they would be if all institutions were required to keep these records for the same period of time?

D. Exception for Limited Information Disclosure When Personnel Leave Their Firms

Finally, we propose to amend Regulation S–P to add a new exception from the notice and opt out requirements to permit limited disclosures of investor information when a registered representative of a broker-dealer or a supervised person of a registered investment adviser moves from one brokerage or advisory firm to another. The proposed exception is intended to allow firms with departing representatives to share limited customer information with the representatives' new firms that could be used to contact clients and offer them a choice about whether to follow a representative to the new firm. At many firms, representatives develop close professional and personal relationships with investors over time. Representatives at such firms likely remember the basic contact information for their clients or have recorded it in their own personal records. Some firms discourage departing representatives from soliciting clients to move to another firm, while others do not. At any firm, departing representatives may have a strong incentive to transfer as much customer information as possible to their new firms, and it has been brought to our attention that, at some firms, information may have been transferred without adequate supervision, in contradiction of privacy notices provided to customers, or potentially in violation of Regulation S–P.[90]

The proposed exception is designed to provide an orderly framework under which firms with departing representatives could share certain limited customer contact information and could supervise the information transfer.[91] The proposed exception would permit one firm to disclose to another only the following information: the customer's name, a general description of the type of account and products held by the customer, and contact information, including address, telephone number and e-mail information.[92] We propose to include this particular information as it would be useful for a representative seeking to maintain contact with investors, but appears unlikely to put an investor at serious risk of identity theft. It also is the type of information an investor would expect a representative to remember. Broker-dealers and registered investment advisers seeking to rely on the exception would have to require their departing representatives to provide to them, not later than the representative's separation from employment, a written record of the information that would be disclosed pursuant to the exception, and broker-dealers and registered investment advisers would be required to preserve such records consistent with the proposed recordkeeping provisions of Section 30.[93] This condition is intended

[88] *See* proposed paragraph (c) of Section 30.

[89] *See* 17 CFR 240.17a–4(b); 240.17Ad–7(b); 270.31a–2(a)(4)–(6); 275.204–2(e)(1).

[90] *See, e.g., In re NEXT Financial Group, Inc., supra* note 16.

[91] In 2004, certain large broker-dealers entered into a protocol under which signatories agreed not to sue one another for recruiting one another's registered representatives, if the representatives take only limited client information to another participating firm. The initial signatories, Citigroup Global Markets/Smith Barney, Merrill Lynch, and UBS Financial Services, were joined more recently by Raymond James, Wachovia Securities and others.

We understand that, under the protocol, the information that a departing representative may take to another firm is limited to each client's name, address, a general description of the type of account and products held by the client, and the client's phone number and e-mail address. This information may be used at the representative's new firm only by the representative, and only for the purpose of soliciting the representative's former clients.

We further understand that there may be some confusion in the securities industry regarding what information may be disclosed to a departing representative's new firm consistent with the limitations in Regulation S–P, and that at times these limitations may cause inconvenience to investors. NASD (now consolidated into FINRA) issued guidance to its member firms regarding the permissible and impermissible use of ''negative response letters'' for bulk transfers of customer accounts and changes in the broker-dealer of record on certain types of accounts (*see* NASD NtM 04–72 (Oct. 2004); NtM 02–57 (Sept. 2002)). More recently, FINRA issued guidance relating to Regulation S–P in the context special considerations firms should use to supervise recommendations of newly associated registered representatives to replace mutual funds and variable products). *See* FINRA, Regulatory Notice 07–36, available at *http://www.finra.org/web/groups/rules_regs/documents/notice_to_members/p036445.pdf*. However, our staff reports that scenarios involving representatives moving from one firm to another continue to create uncertainty regarding firms' obligations under Regulation S–P.

[92] *See* proposed paragraph (a)(8)(i) of Section 15.

[93] *See* proposed paragraph (a)(8)(iii) of Section 15 and proposed paragraph (c) of Section 30. For purposes of the proposed exception, the term ''representative'' would be defined to mean a natural person associated with a broker or dealer registered with the Commission, who is registered or approved in compliance with 17 CFR 240.15b7–

to help ensure that firms relying on the exception are appropriately accounting for the information they are disclosing in connection with departures of their representatives.[94]

The exception would be subject to conditions that are designed to limit the potential that the information would result in identity theft or other abuses. The shared information could not include any customer's account number, Social Security number, or securities positions.[95] A representative would not need this type of information to contact investors, although it would be useful to an identity thief, and an investor probably would not expect a representative to remember it. In addition, a representative could solicit only an institution's customers that were the representative's clients. This condition recognizes that an investor might expect to be contacted by a representative with whom the investor has done business before, but not by another person at the representative's new firm.[96]

As noted above, the proposed exception is designed to facilitate the transfer of client contact information that would help broker-dealers and registered investment advisers offer clients the choice of following a departing representative to a new firm. At firms that choose to rely on it, the proposed exception also should reduce potential incentives some representatives may have to take information with them secretly when they leave. By specifically limiting the types of information that could be disclosed to the representative's new firm, the proposed amendments are designed to help firms safeguard more sensitive client information. This limitation also would clarify that a firm may not require or expect a representative from another firm to bring more information than necessary for the representative to solicit former clients. Because the proposed exception is designed to promote investor choice, provide legal certainty, and reduce potential incentives for improper disclosures, we preliminarily believe that it would be necessary or appropriate in the public interest, and is consistent with the protection of investors.

The proposed exception would not limit the disclosure of additional information to a new firm pursuant to a customer's consent or direction.[97] It also would not preclude the disclosure of additional information required in connection with the transfer of a customer's account.[98] Depending on its business organization, its policies regarding departing representatives and the circumstances of a representative's departure, a firm could choose to rely on existing exceptions rather than the proposed new exception.[99] The proposed exception is designed to allow firms that choose to share limited contact information to do so. The proposed exception would not, however, affect firm policies that prohibit the transfer of any customer information other than at the customer's specific direction.

We have chosen to propose this approach as opposed to an alternative approach that would require all firms to include specific notice and opportunity to opt out of this information sharing in their initial and annual privacy notices. Under this alternative, a broker-dealer or registered investment adviser's privacy notice would have to provide specific disclosure regarding the circumstances under which the broker-dealer or adviser would share customer information with another firm when a registered representative or supervised person leaves. We have chosen this approach because, as indicated earlier, many representatives develop close professional and personal relationships with investors. They are likely to remember basic contact information for their clients or have recorded it in their own personal records, and investors would expect representatives to have this information. This type of limited contact information is unlikely to put investors at serious risk of identity theft. Also, we believe that a description of disclosures to a departing representative's new firm would be difficult to distinguish from the description of disclosures made for the purpose of third-party marketing and would further complicate already complex privacy notices.

- Commenters are invited to discuss the proposed new exception. Would it permit the transfer of contact information so as to promote investor choice and convenience? Would it foreclose the transfer of particularly sensitive information that, if misused, could lead to identity theft? Should the transfer of customer contact information be conditioned on the broker-dealer or registered investment adviser receiving the information certifying to the sharing institution that it complies with the safeguards and disposal rules?
- We also invite commenters to share their views on the likely effect of the proposed new exception on competition in recruiting broker-dealer and investment adviser representatives. Are there alternative approaches that would both protect investor information and not unduly restrict the transfer of representatives from one firm to another?
- We seek comment on potential alternative approaches, including requiring specific disclosure. Are investors, particularly new clients to a firm, likely to understand disclosures about information that would be given to a departing representative's new firm in initial or annual privacy notices? [100] Should the availability of the proposed exemption be conditioned on providing investors with specific disclosure regarding whether a covered institution would disclose personal information in connection with a representative's departure?
- The proposed exception would permit broker-dealers and registered investment advisers to transfer limited

1, or a supervised person of an investment adviser as defined in Section 202(a)(25) of the Investment Advisers Act. *See* proposed paragraph (a)(8)(iv) of Section 15.

[94] Most firms seeking to rely on the proposed exception would not need to revise their GLBA privacy notices because they already state in the notices that their disclosures of information not specifically described include disclosures permitted by law, which would include disclosures made pursuant to the proposed exception and the other exceptions provided in Section 15 of Regulation S–P.

[95] *See* proposed paragraph (a)(8)(ii) of Section 15.

[96] *See* proposed paragraph (a)(8)(i) of Section 15 (permitting a representative to solicit customers to whom the representative personally provided a financial product or service on behalf of the institution).

[97] For example, if an investor chooses to move his or her business to the representative's new firm, he or she may consent to having the original firm disclose additional information about the customer's account to the representative's new firm without the firm first having to provide the customer with an opt out. *See* 17 CFR 248.15(a)(1).

[98] If an investor requests or authorizes the transfer of his or her account from the representative's old firm to the representative's new firm, the old firm may disclose additional information as necessary to effect the account transfer. *See* 17 CFR 248.14(a)(1) and 248.14(b)(2)(vi)(B). The exception also would not preclude the disclosure of additional information about the investor if the firm has provided the investor with a privacy notice describing the disclosure and given the investor a reasonable opportunity to opt out of the disclosure, and the customer has not opted out. *See* 17 CFR 248.10. Thus, covered institutions that wish to disclose an investor's nonpublic personal information to a departing representative's new firm without relying on the proposed new exception or without first obtaining consent from the investor to the disclosure or to an account transfer could revise their privacy notices to describe disclosures the firm would make in the context of a representative's move to another broker-dealer or registered investment adviser.

[99] *See* 17 CFR 248.14, 248.15.

[100] We expect that if the Banking Agencies, the FTC and the Commission were to adopt the proposed model privacy form, *see* Interagency Model Privacy Form Proposal, *supra* note 12, the description of the disclosure to a nonaffiliated firm could be included on page 2 of the proposed form in the section defining nonaffiliates.

information to other broker-dealers and registered investment advisers without first providing notice and opt out. Should we make the proposed exception available for information transferred to other types of financial institutions where a departing representative may go? For example, should we permit broker-dealers and registered investment advisers to rely on the exception to share information with investment advisers that are not registered with the Commission?

• Commenters are invited to express their views on the proposed exemption's condition that a departing representative of a covered institution relying on this exemption could solicit only the institution's customers that were the representative's clients.

III. General Request for Comments

We request comment on all aspects of the proposed amendments to Regulation S–P. We particularly urge commenters to suggest other provisions or changes that could enhance the ways in which securities industry participants protect personal information. We encourage commenters to provide empirical data, if available, to support their views.

IV. Paperwork Reduction Act

Certain provisions of the proposed amendments contain ''collections of information'' requirements within the meaning of the Paperwork Reduction Act of 1995 (''PRA'').[101] The Commission is submitting these amendments to the Office of Management and Budget (''OMB'') for review and approval in accordance with the PRA.[102] The title for the collections of information is ''Information security programs for personal information; records of compliance.'' The safeguards and disposal rules we propose to amend contain currently approved collections of information under OMB Control No. 3235–0610, the title of which is, ''Rule 248.30, Procedures to safeguard customer records and information; disposal of consumer report information.'' [103] The Commission is proposing to amend Regulation S–P's safeguards and disposal rules, 17 CFR 248.30(a) and (b), pursuant to Sections 501, 504, 505, and 504 of the GLBA,[104] Sections 17, 17A, 23, and 36 of the Exchange Act,[105] Sections 31(a) and 38 of the Investment Company Act,[106] and Sections 204 and 211 of the Investment Advisers Act.[107] Regulation S–P sets forth the Commission's safeguards rule for institutions covered by the regulation. Among other things, the safeguards rule requires covered institutions to adopt administrative, technical, and physical information safeguards to protect customer records and information. Regulation S–P also contains the Commission's disposal rule, which requires institutions to properly dispose of consumer report information possessed for a business purpose by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

The proposed amendments are designed to ensure that covered institutions maintain a reasonable information security program that includes safeguarding policies and procedures that are more specific than those currently required, including policies and procedures for responding to data security breach incidents, for notifying individuals for whom the incidents pose a risk of identity theft, and for reporting certain incidents to the Commission (or to a broker-dealer's designated examining authority) on proposed Form SP–30. The amendments also would broaden the scope of information and the types of institutions and persons covered by the safeguards and disposal rules. Finally, the amendments would create a new exception from Regulation S–P's notice and opt-out requirements for disclosures of limited information in connection with the departure of a representative of a broker-dealer or registered investment adviser. Firms choosing to rely on the exception would be required to keep records of the information disclosed pursuant to it.

The hours and costs associated with these collections of information would consist of reviewing the proposed amendments, collecting and searching for existing policies and procedures, conducting a risk assessment, developing and recording information safeguards appropriate to address risks, training personnel, and adjusting written safeguards on an ongoing basis. Institutions would also have to respond appropriately to incidents of data security breach as may occur on an ongoing basis. If misuse of information has occurred or is reasonably possible, this would include notifying affected individuals. If there is a significant risk that an individual identified with the information might suffer substantial harm or inconvenience, or any unauthorized person has intentionally obtained access to or used sensitive personal information, this would also include notifying the Commission or an appropriate designated examining authority as soon as possible on proposed Form SP–30. Certain of these collections of information also would require disclosure, reporting, and recordkeeping burdens, as analyzed below.

An agency may not conduct or sponsor, and a person is not required to respond to a collection of information unless a currently valid OMB control number is displayed. Responses to these collections of information would not be kept confidential.[108] The collections of information would be mandatory, and would have to be maintained by broker-dealers for not less than three years, the first two years in an easily accessible place, by registered transfer agents for a period of not less than two years, the first year in an easily accessible place, by investment companies for a period not less than six years, the first two years in an easily accessible place, and registered investment advisers would have to preserve the records for five years, the first two years in an appropriate office of the investment adviser.

Information Security and Security Breach Response Requirements

The proposed amendments contain collections of information requirements related to the more specific standards we are proposing for safeguarding personal information, including standards for responding to data security breaches. We believe these proposed collections of information are necessary to help prevent and address security breaches and designed to ensure that covered institutions maintain a reasonable information security program pursuant to the statutory requirements. Covered institutions would have to document in writing steps they would be required to take to develop, implement, and maintain a comprehensive information security program. We estimate that there would be 12,432 respondents to this information collection.[109] Of these

[101] 44 U.S.C. 3501–3520.

[102] 44 U.S.C. 3507(d) and 5 CFR 1320.11.

[103] The paperwork burden imposed by Regulation S–P's notice and opt-out requirements, 17 CFR 248.1 to 248.18, is currently approved under a separate OMB control number, OMB Control No. 3235–0537. The proposed amendments would not affect this collection of information.

[104] 15 U.S.C. 6801, 6804, 6805 and 6825.

[105] 15 U.S.C. 78q, 78q–1, 78w, and 78mm.

[106] 15 U.S.C. 80a–30(a), 80a–37.

[107] 15 U.S.C. 80b–4, 80b–11.

[108] Information submitted to the Commission on proposed Form SP–30 would be kept confidential to the extent permitted by law. *See supra* note 55.

[109] This estimate includes 6,016 broker-dealers, 4,733 investment companies representing portions of 813 fund complexes, 77 business development companies, 9,860 registered investment advisers, and 501 registered transfer agents. As discussed in

covered institutions, we estimate that 5,862 are smaller institutions and 6,570 are larger institutions. [110]

Based on limited inquiries of covered institutions, the staff estimates that the amount of time smaller institutions would devote to initial compliance with the proposed amendments would range from 2 to 80 hours with a midpoint of 41 hours.[111] This estimate reflects the following burden hours: 1 hour for the board of directors to designate an information security program coordinator; 1 hour for the program coordinator to review the amendments; 4 hours to assess risks and review procedures; 10 hours to review, revise and implement new safeguards (including any data breach notification procedures); 8 hours to test the effectiveness of the safeguards controls and procedures; 7 hours to train staff; and 10 hours to review service providers' policies and procedures and revise contracts as necessary to require them to maintain appropriate safeguards. The staff estimates that initially it would cost smaller institutions approximately $18,560 to comply with the proposed amendments.[112] Amortized over three years, the estimated annual hourly burden would be 14 hours at a cost of approximately $6,187.

The staff estimates that the amount of time larger institutions would devote to initial compliance with the proposed amendments would range from 40 hours to 400 hours with a midpoint of 220 hours.[113] This estimate reflects the following burden hours: 2 hours for the board of directors to designate an information security program coordinator; 2 hours for the program coordinator to review the amendments; 42 hours to assess risks and review procedures; 60 hours to review, revise and implement new safeguards (including any data breach notification procedures); 60 hours to test the effectiveness of the safeguards controls and procedures; 34 hours to train staff; and 20 hours to review service providers policies and procedures and revise contracts as necessary to require them to maintain appropriate safeguards. The staff estimates that larger institutions would spend approximately $172,732 to comply with the proposed amendments initially.[114] Amortized over three years, the estimated annual hourly burden would be 73 hours at a cost of approximately $57,577.

On an annual, ongoing basis the staff estimates that the amount of time smaller institutions would devote to ongoing compliance with the safeguards and disposal rules, as they are proposed to be amended, would range from 12 hours to 40 hours per year with a midpoint of 26 hours per year. This estimate reflects the following burden hour estimates: 5 hours to regularly test or monitor the safeguards' key controls, systems, and procedures; 3 hours to augment staff training; 3 hours to provide continued oversight of service providers; 3 hours to evaluate and adjust safeguards; 10 hours to respond appropriately to potential incidents of data security breach, including investigating the breach and, as necessary, notifying affected individuals; and 2 hours to notify the Commission or a designated examining authority as soon as possible on proposed Form SP–30, in the event there is a significant risk that an individual identified with the information might suffer substantial harm or inconvenience or an unauthorized person has intentionally obtained access to or used sensitive personal information.[115] We believe that most institutions investigate data security breaches as a matter of good business practice to protect their business operations and the sensitive information they have about employees and clients. Nevertheless, we have estimated additional burden hours because the proposed rule specifies certain elements of the investigation and the notice to affected individuals. We also believe that an institution would have gathered all the information that would have to be disclosed in Form SP–30 in the course of these investigations of data security breaches. Thus, staff estimates for the Form SP–30 collection of information burden reflect only the time it would take to draft the information on the form. Staff estimates that smaller institutions would spend an additional $10,764 per institution per year in connection with these burdens.[116]

The staff also estimates that the amount of time larger institutions would

more detail in the cost-benefit analysis below, the staff estimates that 56 percent of these 17,267 institutions, or 9,670 institutions, have one or more affiliates. The staff estimates, for purposes of this analysis, that each of the affiliated institutions has one corporate affiliate. The staff estimates that these affiliated institutions are likely to bear these paperwork burdens on an organization-wide basis, rather than being incurred by each institution. Based on these estimates, the staff estimates there would be 12,432 respondents to this information collection. (17,267 − (9,670 ÷ 2) = 12,432) These estimates are discussed in more detail in the cost-benefit analysis, *see infra* note 149 and accompanying text.

[110] *See infra* note 154 and accompanying text.

[111] The staff estimate uses the midpoint of the range of hours, although the average number of burden hours could be higher or lower. Our estimates are based on staff contacts with several institutions regarding their current safeguarding and disposal policies and procedures as well as the potential costs of the proposed amendments. Because the staff was able to discuss these issues with only a small number of very large institutions, and our estimates in this analysis are based largely on this information, our estimates may be much higher or lower than the range of actual current costs related to compliance with Regulation S–P and the range of potential costs associated with the proposed amendments.

[112] This estimate is based on a cost of $2,000 for one hour of the board of directors' time (at $2,000/hour) and $16,560 for 40 hours of a program coordinators' time (at $414/hour). Staff believes that the program coordinator would be a senior executive of the institution, such as a chief compliance officer of an investment adviser. For purposes of this PRA analysis, the staff is using salaries for New York-based employees which tend to be higher than the salaries for comparable positions located outside of New York. This conservative approach is intended to capture unforeseen costs and to account for the possibility that a substantial portion of the work would be undertaken in New York. The salary information is derived from data compiled by the Securities Industry and Financial Markets Association. The Commission staff has modified this information to account for an 1,800-hour work year and multiplied by 5.35 to account for bonuses, firm size, employee benefits, and overhead. *See* Securities Industry and Financial Markets Association, *Report on Management and Professional Earnings in the Securities Industry* (2007); Securities Industry and Financial Markets Association, *Report on Office Salaries in the Securities Industry* (''SIFMA Earnings Reports'').

[113] The staff estimate uses the midpoint of the range of hours, although the average number of burden hours could be higher or lower.

[114] This estimate is based on a cost of $4,000 for 2 hours of board of directors' time (at $2,000/hour) and $168,732 for 218 hours of a group of compliance professionals' time (at $774/hour). The staff believes that this group of compliance professionals would include the program coordinator at a rate of $414 per hour, an in-house attorney at a rate of $295 per hour, and an administrative assistant at a rate of $65 per hour. *See* SIFMA Earnings Reports, *supra* note 112. In total, we estimate that this group of compliance professionals would cost the larger institution $758 per hour. $414 + $295 + $65 = $774.

[115] We estimate that each covered institution that has developed and adopted and is maintaining safeguarding policies and procedures will experience some form of breach of data security each year. *See, e.g.*, Deloitte & Touche LLP and Ponemon Institute LLC, Enterprise@Risk: 2007 Privacy & Data Protection Survey (Dec. 2007), *http://www.deloitte.com/dtt/cda/doc/content/us_risk_s%26P_2007%20Privacy10Dec2007final.pdf* (last visited Dec. 19, 2007) (85% of surveyed privacy and security professionals experienced a reportable breach within the past 12 months). These data security breaches may range from minor breaches (such as an individual who accidentally sees data that he or she does not have authority to view) to more serious breaches. Accordingly, we have estimated that each of these institutions would experience a data security breach that would require notice to the Commission (or a designated examining authority) each year. We understand that the nature of security breaches will vary widely within and among institutions, and that this estimate may be much higher than the actual reporting that would be required under the proposed rule.

[116] This estimate is based on the following calculation: 26 hours per smaller institution per year × $414 per hour = $10,764.

devote to ongoing compliance with the proposed amendments would range from 32 hours to 100 hours with a midpoint of 66 hours per year. This estimate reflects the following burden hour estimates: 12 hours to regularly test or monitor the safeguards' key controls, systems, and procedures; 9 hours to augment staff training; 9 hours to provide continued oversight of service providers; 10 hours to evaluate and adjust safeguards; 20 hours to respond appropriately to potential incidents of data security breach, including investigating the breach and, as necessary, notifying affected individuals; and 6 hours to notify the Commission or a designated examining authority as soon as possible on proposed Form SP–30, in the event there is a significant risk that an individual identified with the information might suffer substantial harm or inconvenience or an unauthorized person has intentionally obtained access to or used sensitive personal information.[117] Staff believes that larger institutions are likely to have more complex business operations and data systems and may experience more sophisticated security attacks than smaller institutions. As a result, staff anticipates that larger institutions are more likely to conduct more complicated investigations that require more detailed explanations on proposed Form SP–30. Staff estimates therefore that larger institutions would take more time to perform investigations and to complete the questions on proposed Form SP–30.[118] The staff estimates that larger institutions would spend approximately an additional $51,084 per institution per year.[119]

Given the estimates set forth above, we estimate that the weighted average initial burden for each respondent would be approximately 136 hours [120] and $100,036.[121] We also estimate that the weighted average ongoing burden for each respondent would be approximately 47 hours [122] and $32,072.[123]

Scope of the Safeguards and Disposal Rules

The amendments also would broaden the scope of information and of the entities covered by the safeguards and disposal rules. These amendments do not contain collections of information beyond those related to the information security and security breach response requirements, analyzed above.

Records of Compliance

The proposed amendments would require that written records required under the disposal and safeguards rules be maintained and preserved by broker-dealers for not less than three years, the first two years in an easily accessible place, by registered transfer agents for a period of not less than two years, the first year in an easily accessible place, by investment companies for a period not less than six years, the first two years in an easily accessible place, and registered investment advisers would have to preserve the records for five years, the first two years in an appropriate office of the investment adviser. Covered institutions are already required pursuant to other Commission rules to maintain and preserve similar records in the same manner, and we do not believe that the currently approved collections of information for these rules would change based on the proposed amendments.[124]

Exception for Limited Information Disclosure When Personnel Leave Their Firms

The proposed amendments would create a new exception from Regulation S–P's notice and opt out requirements that would permit limited disclosures of investor information when a registered representative of a broker-dealer or supervised person of a registered investment adviser moves from one brokerage or advisory firm to another. This exception would require that the departing representative provide the broker, dealer, or registered investment adviser he or she is leaving with a written record of the permissible information that would be disclosed under this exception. Broker-dealers and registered investment advisers also would be required to retain a record of that information consistent with existing record retention requirements. All broker-dealers and registered investment advisers maintain records of their customers and clients, including relevant contact information and type of account. Thus, we estimate that allowing a departing representative to make a copy of this information and requiring the broker-dealer or registered investment adviser to retain a record of that information would not result in an additional measurable burden to the firm.

We request comment on whether these estimates are reasonable. Pursuant to 44 U.S.C. 3506(c)(2)(B), the Commission solicits comments in order to: (i) Evaluate whether the proposed collections of information are necessary for the proper performance of the functions of the Commission, including whether the information will have practical utility; (ii) evaluate the accuracy of the Commission's estimate of the burden of the proposed collections of information; (iii) determine whether there are ways to enhance the quality, utility, and clarity of the information to be collected; and (iv) minimize the burden of the collections of information on those who are to respond, including through the use of automated collection techniques or other forms of information technology.

Members of the public may direct to us any comments concerning the accuracy of these burden estimates and any suggestions for reducing these burden hours. Persons wishing to submit comments on the collection of information requirements of the proposed amendments should direct them to the Office of Management and Budget, Attention Desk Officer of the Securities and Exchange Commission, Office of Information and Regulatory Affairs, Room 10102, New Executive Office Building, Washington, DC 20523, and should send a copy to Nancy M. Morris, Secretary, Securities and Exchange Commission, 100 F Street, NE., Washington, DC 20549–1090 with reference to File No. S7–06–08. OMB is required to make a decision concerning the collections of information between 30 and 60 days after publication of this release; therefore a comment to OMB is best assured of having its full effect if OMB receives it within 30 days after the publication of this release. Requests for materials submitted to OMB by the Commission with regard to these collections of information should be in writing, refer to File No. S7–06–08, and be submitted to the Securities and Exchange Commission, Public Reference

[117] *See supra* note 115.

[118] We recognize that the time it takes to perform an investigation of a data security breach and to complete Form SP–30 may vary significantly depending on the nature, size and complexity of an institution's business operations as well as the nature and size of the security breach. Accordingly, the actual time it may take a particular institution to investigate the breach and complete Form SP–30 may vary significantly from staff estimates.

[119] This estimate is based on the following calculation: 66 hours × $774 = $51,084.

[120] This estimate is based on the following calculation: ((5,862 smaller institutions × 41 hours) + (6,570 larger institutions × 220 hours) ÷ 12,432 total institutions = 135.60 hours.

[121] This estimate is based on the following calculation: ((5,862 smaller institutions × $18,560) + (6,570 larger institutions × $172,732)) ÷ 12,432 total institutions = $100,036.03.

[122] This estimate is based on the following calculation: ((5,862 smaller institutions × 26 hours) + (6,570 larger institutions × 66 hours)) ÷ 12,432 total institutions = 47.14 hours.

[123] This estimate is based on the following calculation: ((5,862 smaller institutions × $10,764) + (6,570 larger institutions × $51,084)) ÷ 12,432 total institutions = $32,072.12.

[124] *See* 17 CFR 240.17a–4(b); 240.17Ad–7(b); 270.31a–2(a)(4)–(6); 275.204–2(e)(1).

Room, 100 F Street, NE., Washington, DC 20549.

V. Cost-Benefit Analysis

The Commission is sensitive to the costs and benefits imposed by its rules. We have identified certain costs and benefits of the proposed amendments and request comment on all aspects of this cost-benefit analysis, including identification and assessment of any costs and benefits not discussed in this analysis. We seek comment and data on the value of the benefits identified. We also welcome comments on the accuracy of the cost estimates in each section of this analysis, and request that commenters provide data so we can improve these cost estimates. In addition, we seek estimates and views regarding these costs and benefits for particular covered institutions, including registered transfer agents, as well as any other costs or benefits that may result from the adoption of these proposed amendments.

As discussed above, the proposed rule amendments are designed to enhance covered institutions' information security policies and procedures as well as their ability to protect personal information. Under Regulation S–P, covered institutions have been required to safeguard customer records and information since 2001 and to dispose properly of consumer report information since 2005. The proposed amendments would modify Regulation S–P's current safeguards and disposal rules to: (i) Require more specific standards under the safeguards rule, including standards that would apply to data security breach incidents; (ii) broaden the scope of information and the types of institutions and persons covered by the rules; and (iii) require covered institutions to maintain written records of their policies and procedures and their compliance with those policies and procedures. The proposed amendments also would create a new exception from Regulation S–P's notice and opt-out requirements that would not unduly restrict the transfer of representatives from one broker-dealer or registered investment adviser to another while protecting customer information.

A. Costs and Benefits of More Specific Information Security and Security Breach Standards

As noted, since 2001 broker-dealers, investment companies, and registered investment advisers have been required to adopt policies and procedures reasonably designed to insure the security and confidentiality of customer records and information, protect against anticipated threats or hazards, and protect against unauthorized access to or use of customer records and information.[125] The proposed rule amendments would require more specific standards for safeguarding personal information, including standards for responding to data security breaches. The amendments would require covered institutions to develop, implement, and maintain a comprehensive ''information security program'' for protecting personal information and for responding to unauthorized access to or use of personal information that would have to be appropriate to the institution's size and complexity, the nature and scope of its activities, and the sensitivity of the personal information involved. The information security program would have to include seven safeguarding elements, as described above in section II.A. Our proposed amendments also would specifically require that institutions' information security programs include procedures for responding to incidents of unauthorized access to or use of personal information. We believe that these proposed amendments would be consistent with safeguarding guidance and rules issued by the Banking Agencies and the FTC.[126]

1. Benefits of More Specific Information Security and Security Breach Standards

We anticipate that the proposed amendments would benefit covered institutions and investors by providing specific standards for policies and procedures to safeguard investor information, boosting investor confidence and mitigating losses due to security breach incidents, helping to ensure that information security programs are actively managed and regularly updated, and reducing the compliance burden for institutions in the event of a data security breach incident.

One benefit of the proposed information security and security breach standards would be to provide firms in the securities industry with detailed standards for the policies and procedures that a well-designed information security program should include. As already noted, a significant increase in reported information security breaches involving covered institutions, including increasingly sophisticated identity theft attacks directed at the securities industry, have altered the risk environment and brought to our attention the vulnerability of certain of our institutions' information security policies and procedures.[127] We are concerned that some Commission-regulated institutions may not regularly reevaluate and update their safeguarding programs to deal with these increasingly sophisticated methods of attack. As a result, our staff has devoted increased attention to this area.

The current rule's reasonable design standard has permitted institutions flexibility to implement safeguarding policies and procedures tailored to their own privacy policies and practices and their varying business operations. While many institutions have appropriate safeguards in place, some institutions, including some smaller institutions, may have had difficulty keeping up with the changes in the threat environment. Setting out a more specific framework for institutions' continuing obligation to protect customer information, may ease institutions' burden in interpreting our expectations of safeguarding policies and procedures that are ''reasonably designed,'' while retaining much of the current rule's flexibility.

We believe the proposed amendments would be consistent with the Commission's initial statutory mandate under the GLBA to adopt, in 2000, final financial privacy regulations that are consistent and comparable with those adopted by other federal financial regulators.[128] As noted above, after our adoption of Regulation S–P's safeguards rule, the FTC and the Banking Agencies issued regulations with more detailed standards applicable to the institutions they regulate.[129] The Banking Agencies also issued guidance for their institutions on responding to incidents of unauthorized access to or use of customer information.[130] Our proposed amendments include safeguarding elements consistent with the regulatory provisions of these other agencies that Commission-regulated institutions would have to address in their safeguarding policies and procedures.[131]

---

[125] *See* 15 U.S.C. 6801; 17 CFR 248.30(a). The Commission also required that safeguarding policies and procedures be in writing by July 1, 2005. *See* Disposal Rule Adopting Release, *supra* note 15.

[126] *See supra* note 23 and accompanying text.

[127] *See supra* notes 16–19 and accompanying text.

[128] *See* Section 504(a) of the GLBA (15 U.S.C. 6804(a)).

[129] *See supra* note 23 and accompanying text.

[130] *Id.*

[131] When the FTC adopted its safeguards rule, it stated that an entity that demonstrated compliance with the Banking Agencies' or NCUA's safeguarding standards also would satisfy the FTC rule. The FTC stated, however, that it would not automatically recognize an institution's compliance with other safeguards rules (including Regulation S–P) as satisfying the FTC Safeguards Rule. The FTC stated

Continued

Covered institutions would benefit from having specific standards that are consistent and comparable to those already adopted by the Banking Agencies and the FTC in other ways. For example, covered institutions that have banking affiliates may have already developed policies and procedures consistent with the Banking Agencies' guidance that are applied to all affiliates of the bank. If they do not have the same policies and procedures, these covered institutions would be able to apply the banking affiliate's policies and procedures to the securities businesses with few changes. More specific safeguarding standards also could increase investor confidence in institutions and help mitigate losses that can result from lax safeguarding policies and procedures. Incidents of identity theft have affected a large number of Americans and are difficult and expensive for victims to deal with and correct.[132] Moreover, there is at least anecdotal evidence that the wave of widely-reported incidents of data security breaches have played a role in discouraging a significant number of individuals from conducting business online.[133] The proposed amendments could benefit investors and increase their confidence by providing firms with detailed standards for the processes that a well-designed information security program should include. This could result in enhanced protection for the privacy of investor information, and could decrease incidents of identity theft, thereby mitigating losses due to identity theft and other misuses of sensitive information. We also believe that the increased protection that could result from the proposed amendments could benefit institutions, which frequently incur the costs of fraudulent activity.[134] Thus, if only a small number of security breach incidents were averted because the proposed amendments were adopted, there still could be a significant cost savings to individuals and institutions.[135]

As noted above, we are concerned that some institutions do not regularly reevaluate and update their safeguarding programs. Requiring covered institutions to designate in writing an employee or employees to coordinate their information security programs should foster clearer delegations of authority and responsibility, making it more likely that an institution's programs are regularly reevaluated and updated. Having an information security program coordinator also could contribute to an institution's ability to meet its affirmative and continuing obligation under the GLBA to safeguard customer information.[136] If, for example, elements of a covered institution's information security program were not maintained on a consolidated basis, but were dispersed throughout an institution, we believe having a responsible program coordinator or coordinators should facilitate the institution's awareness of these elements, as well as enable it to better manage and control risks and conduct ongoing evaluations.

We expect that the proposed framework for the initial and ongoing oversight of institutions' information security programs—in the form of formal risk assessments, periodic testing or monitoring of key controls, systems, and procedures, staff training, and relevant evaluations and adjustments—would help to ensure that information security programs are appropriately updated along with relevant changes in technology, new business arrangements, changes in the threat environment, and other circumstances. Finally, the proposed amendment that would require covered institutions to take reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards and would require service providers by contract to implement and maintain appropriate safeguards should help to ensure that sensitive personal information is protected when it leaves the institution's custody, while still permitting institutions the flexibility to select appropriate service providers.

The proposed requirement that information security programs include specific procedures for responding to incidents of unauthorized access to or use of personal information is designed to benefit investors and institutions. The requirement would benefit investors who receive notice of an information security breach pursuant to an institution's incident response procedures by allowing those investors to take precautions to the extent they believe necessary.[137] The procedures also would benefit institutions by establishing a national data breach notification requirement for covered institutions.[138] Currently at least 39 states have enacted statutes requiring notification of individuals in the event of a data security breach.[139] This patchwork of overlapping and sometimes inconsistent regulation has created a difficult environment for financial institutions' compliance programs. However, many of the state statutes contain exemptions for entities regulated by federal data security breach regulations.[140] Accordingly, the proposed amendments could benefit covered institutions by significantly reducing the number of requirements with which covered institutions must

that it made this decision because ''such other rules and law do not necessarily provide comparable protection in terms of the safeguards mandated, data covered, and range of circumstances to which protection apply.'' *See Standards for Safeguarding Customer Information*, 67 FR 36484 (May 23, 2003), at text accompanying and following nn.28–33. Compliance with other Regulation S–P provisions, however, currently satisfies other FTC privacy requirements. Thus, we expect that making the safeguarding provisions of Regulation S–P comparable to the FTC's requirements would benefit institutions by, for example, permitting state-registered investment advisers to satisfy the FTC standards by complying with the Commission's safeguards rule, which was drafted to address investment advisory business models.

[132] In 2003 the FTC reported that up to 10 million Americans had been victimized by identity theft over a 12-month period and that these thefts cost businesses and consumers over $52 billion. *See* FTC, Identity Theft Survey Report (Sept. 2003), available at *http://www.ftc.gov/os/2003/09/synovatereport.pdf*.

[133] A July 2005 study found that 48 percent of consumers avoided making purchases on the Internet because they feared their personal information may be stolen. *See* Cyber Security Industry Alliance, Internet Voter Survey, at 9 (June 2005), *https://www.csialliance.org/publications/surveys_and_polls/CSIA_Internet_Security_Survey_June_2005.pdf* (last visited Nov. 6, 2007).

[134] In most cases, financial institutions do not impose the losses associated with fraudulent activity on consumers. *See, e.g.*, Testimony of Oliver I. Ireland, on Behalf of the Financial Services Coordinating Council, H.R. 3997, the ''Financial Data Protection Act of 2005,'' Before the Subcomm. on Financial Institutions and Consumer Credit, House Comm. on Financial Services (Nov. 9, 2005), available at *http://www.sia.com/testimony/2005/ireland11-9-05.html*.

[135] One research institution has estimated that the average cost of a data security breach incident per institution is $1.4 million. *See* Ponemon Institute, LLC, 2006 Annual Study: Cost of a Data Breach (Oct. 2006), *http://download.pgp.com/pdfs/Ponemon2-Breach-Survey_061020_F.pdf* (last visited Nov. 6, 2007). In addition, some investigations into data breach incidents have been reported to cost as much as $5 million. *See* Daniel Wolfe, Security Watch, Amer. Banker (Apr. 4, 2007).

[136] *See* 15 U.S.C. 6801(a).

[137] Often victims of identity theft are unaware of the crime until they are denied credit or employment, or are contacted by a debt collector for payment on a debt they did not incur. *See* Identity Theft Task Force, Combating Identity Theft, A Strategic Plan, p. 3 (Apr. 2007), available at *http://www.idtheft.gov/reports/StrategicPlan.pdf*.

[138] Establishing national standards for data breach notification requirements was a recommendation of the Identity Theft Task Force. *Id.* at p. 35.

[139] *See* Government Accountability Office, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown (Jun. 4, 2007) at p. 2, and National Conference of State Legislatures, State Security Breach Notification Laws (as of Dec. 1, 2007), *http://www.ncsl.org/programs/lis/cip/priv/breachlaws.htm* (last visited Dec. 10, 2007).

[140] *See, e.g.*, Crowell & Moring LLP, State Laws Governing Security Breach Notification (last updated Apr. 2007), *http://www.crowell.com/pdf/SecurityBreachTable.pdf* (last visited Dec. 10, 2007).

comply.[141] As noted, the banking regulators published similar data breach notification guidance in 2005.[142]

We request comment on available metrics to quantify these benefits and any other benefits the commenter may identify. In particular, we request comment reflecting institutions' experiences in safeguarding customer information and addressing the security breach incidents discussed above. Commenters are also requested to identify sources of empirical data that could be used for the metrics they propose.

2. Costs of More Specific Information Security and Security Breach Standards

Some institutions would likely incur additional costs in reviewing, implementing, and maintaining more specific information security and security breach standards. Institutions could incur additional costs in reviewing current safeguarding policies and procedures and designing and implementing new ones, if necessary, on an initial basis. Institutions also could incur additional costs on an ongoing basis to maintain up-to-date information security programs and to respond appropriately to any data security breach incidents.

According to Commission filings, approximately 6,016 broker-dealers, 4,733 investment companies comprising portions of 813 fund complexes,[143] 77 business development companies, 9,860 registered investment advisers, and 501 registered transfer agents, or 17,267 covered institutions, would be required to comply with the proposed amendments' more specific information security and security breach standards.[144] As noted, broker-dealers, investment companies, and registered investment advisers have been required to have reasonably designed safeguarding policies and procedures since 2001. In addition, transfer agents have been required to have information security safeguards since 2003, in accordance with the FTC Safeguards Rule.[145] We estimate that 56 percent of all covered institutions, or 9,670 institutions, have one or more financial affiliates (whether these institutions are regulated by the Commission or other federal financial regulators).[146] We estimate that each of the affiliated institutions has one corporate affiliate. Based on limited inquiries of covered institutions, we believe that these affiliated institutions are likely to have developed safeguarding policies and procedures on an organization-wide basis, rather than each affiliate developing policies and procedures on its own.[147] We also believe that the affiliate that developed the affiliated organization's safeguarding policies and procedures is also responsible for maintaining these policies and procedures. We therefore estimate that one-half of the covered affiliated institutions, or 4,835 institutions, have developed, documented, and are maintaining safeguarding policies and procedures, while the other half instead use the policies and procedures developed, documented, and maintained by their affiliate.[148] Accordingly, we estimate that 12,432 covered institutions have developed and adopted safeguarding policies and procedures and are maintaining these policies and procedures in accordance with the current rule.[149]

We expect that these institutions' current costs to maintain safeguarding policies and procedures in compliance with the Commission's safeguards rule vary greatly depending upon the size of the institution, its customer base, the complexity of its business operations, and the extent to which the institution engages in information sharing. Thus, for example, we estimate that small investment advisers with fewer than 10 employees require more limited safeguarding policies and procedures to address a limited scope of information transfer, storage, and disposal. We believe that larger broker-dealers or fund complexes, by contrast, are more likely to have and maintain a more extensive set of information safeguarding policies and procedures, corresponding to these institutions' more complex business activities and information sharing practices.

Of the covered institutions, we estimate that 7,030 registered investment advisers have 10 or fewer employees.[150] We estimate that 942 broker-dealers and investment company complexes are small institutions, and are likely to have no more than 10 employees.[151] Based on Commission filings, we also estimate that 170 transfer agents are smaller institutions that are likely to have no more than 10 employees. We therefore estimate that 8,142 institutions, out of 17,267 covered institutions, are smaller institutions that are likely to have no more than 10 employees.[152] We believe that the institutions that have developed and adopted safeguarding policies and procedures are as likely to be smaller institutions with no more than 10 employees as the total population of covered institutions.[153] Therefore, of 12,432 covered institutions that we estimate have developed and adopted and are maintaining safeguarding policies and procedures, we estimate for purposes of this analysis that 5,862 institutions are smaller institutions,

[141] Under the proposed amendments, for example, using proposed Form SP–30 would satisfy an institution's obligations to notify the Commission or the appropriate designated examining authority. Because many state laws have exceptions from breach notification requirements for institutions subject to federal breach notification requirements, this would streamline institutions' current reporting obligations to numerous state authorities.

[142] *See* Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, 70 FR 15736 (Mar. 29, 2005), available at *http://www.occ.treas.gov/consumer/Customernoticeguidance.pdf.* The guidance supplements the Interagency Guidelines Establishing Standards for Safeguarding Information which was renamed the Interagency Guidelines Establishing Information Security Standards.

[143] Although the circumstances for every investment company vary, we believe that in general the costs of complying with the proposed rule amendments would be incurred on a per fund complex basis and not on a per fund basis because almost all investment companies are externally managed by affiliated organizations and independent contractors, who, if the proposals are adopted, are likely to review and implement the amended rules on behalf of all of the investment companies they manage. *See, e.g.,* Investment Company Institute, A Guide to Understanding Mutual Funds, at 16, Sept. 2006, available at *http://www.ici.org/pdf/bro_understanding_mfs_p.pdf* (last visited Dec. 3, 2007). Thus, throughout this cost-benefit analysis we estimate the costs of compliance on a per fund complex basis.

[144] This estimate is based on the following calculation: 6,016 + 813 + 77 + 9,860 + 501 = 17,267.

[145] *See supra* note 23.

[146] The estimate that 56 percent of registrants have an affiliate is based upon statistics reported as of December 3, 2007 on Form ADV, the Universal Application for Investment Adviser Regulation, which contains specific questions regarding affiliations between investment advisers and other persons in the financial industry. We estimate that other institutions subject to the safeguards rule would report a rate of affiliation similar to that reported by registered investment advisers. The estimate that 9,670 institutions have an affiliate is based on the following calculation: 17,267 × 0.56 = 9,669.52.

[147] *See supra* note 109.

[148] *This estimate is based on the following calculation:* 9,670 ÷ 2 = 4,835.

[149] *This estimate is based on the following calculation:* (17,267 − 9,670) + 4,835 = 12,432.

[150] *See* Investment Adviser Association, Evolution Revolution, A Profile of the Investment Adviser Profession (2006), available at *http://www.nrs-inc.com/ICAA/EvRev06.pdf.*

[151] As noted below, 915 broker-dealers and 238 investment companies, representing 27 fund complexes, are small entities.

[152] *This estimate is based on the following calculation:* 7,030 + 942 + 170 = 8,142 smaller institutions.

[153] 8,142 ÷ 17,267 = 0.4715.

while 6,570 institutions are larger institutions.[154]

Based on conversations with representatives of covered institutions, and information collected from limited inquiries of covered institutions, we estimate that smaller institutions are currently spending between $5,000 and $1,000,000 per year to comply with the safeguards and disposal rules.[155] We also estimate that larger institutions are spending between $200,000 and $10,000,000 per year to comply with the safeguards and disposal rules. These estimates include costs for dedicated personnel, maintaining up-to-date policies and procedures, enforcing various safeguarding requirements (such as ''clean desk'' requirements), hiring contractors to properly dispose of sensitive information, developing and enforcing access procedures, ongoing staff training, monitoring and reviewing compliance with safeguarding standards, and computer encryption. These estimates also include current spending to comply with state data security breach statutes.[156]

We expect that most covered institutions have information security programs in place that would be consistent with the proposed amendments.[157] We do not have a reliable basis for estimating the number of institutions that would incur additional costs or the extent to which those institutions would have to enhance their policies and procedures, including documentation of the information safeguard program and its elements. Accordingly, we have estimated the range of additional costs that individual firms could incur. We seek comment on the number of firms that have information safeguard programs that would satisfy the proposed amendments, the number of firms that would have to enhance their programs, the extent of those enhancements, and the costs of enhancement.

If the proposed amendments were adopted, covered institutions could incur costs to supplement their current information security programs in some or all of the following ways. First, the institution would be required to review and, as appropriate, revise its current safeguarding policies and procedures, including their data security breach procedures and disposal rule procedures, to comply with the more specific requirements of the proposed amendments. Initially this would require the institutions to: (i) Designate an employee or employees as coordinator for the information security program; (ii) identify in writing reasonably foreseeable security risks that could result in the unauthorized access or compromise of personal information or personal information systems; (iii) review existing or design new safeguards to control these risks; (iv) train staff to implement the safeguards; and (v) test the effectiveness of the safeguards' key controls, including access controls, controls to detect, prevent and respond to incidents of unauthorized access to or use of personal information. Second, an institution also would be required to review its service providers' information safeguards and determine whether its service providers are capable of maintaining appropriate safeguards for personal information, document this finding, and enter into contracts with the service providers to implement and maintain appropriate safeguards.

Third, an institution would be required to review existing safeguarding procedures relating to data security breach incidents. Initially, this could include: (i) Assessing current policies and procedures for responding to data breach incidents; and (ii) designing and implementing written policies and procedures to assess, control, and investigate incidents of unauthorized access or use of sensitive personal information, as well as policies and procedures to notify individuals and the Commission or a broker-dealer's designated examining authority, if necessary.

Fourth, to comply with these amendments on an ongoing basis, institutions would be required to: (i) Regularly test or monitor, and maintain a written record of the effectiveness of their safeguards' key controls, systems and procedures (including an assessment of personal information system access controls, controls designed to detect, prevent and respond to data security breach incidents, and controls related to employee training or supervision); (ii) train staff to implement their information security program; (iii) continue and document their oversight of service providers; and (iv) evaluate and adjust their information security programs in light of testing and monitoring, and changes in technology, business operations or arrangements, and other material circumstances.

Finally, an institution would be required to begin to respond to any data security breach incidents as may occur on an ongoing basis. This would include implementing and following written procedures to: (i) Assess the nature and scope of the incident; (ii) take appropriate steps to contain and control it, and document those steps in writing; (iii) promptly conduct a reasonable investigation and make a written determination of the likelihood that sensitive personal information had been or would be misused; (iv) if misuse of information had occurred or were reasonably likely, notify affected individuals; and (v) if an individual identified with the information had suffered substantial harm or inconvenience, or any unauthorized person had intentionally obtained access to or used sensitive personal information, notify the Commission, or the appropriate designated examining authority as soon as possible on proposed Form SP–30.

We expect these estimated costs would vary significantly depending on the size of the institution, the adequacy of its existing safeguarding policies and procedures, and the nature of the institution's operations. The ''reasonably designed'' standard for information security programs in the proposed rule amendments is consistent with the current safeguards and disposal rules. Thus, we believe it should be relatively straightforward for an institution that does not currently have policies and procedures that apply to specific elements of the proposed amendments to incorporate these elements into its current system of safeguarding policies and procedures. In addition, we estimate that little or no modification to an institution's safeguarding policies and procedures would be required in situations where a covered institution's affiliate developed

---

[154] $12,432 \times 0.4715 = 5,861.88$; $12,432 - 5,862 = 6,570$.

[155] *See supra* note 111.

[156] These estimates also include transfer agents' current spending to comply with the FTC Safeguards Rule. As noted, the proposed amendments would apply to every broker or dealer other than a notice-registered broker or dealer, every investment company, and every investment adviser or transfer agent registered with the Commission. *See* proposed paragraph (a)(1) of Section 30.

[157] This belief is consistent with the analysis of the Office of the Comptroller of the Currency and Office of Thrift Supervision when they adopted the Banking Agencies Safeguard Guidelines in 2001. At that time they stated with respect to the institutions they regulated, that ''most if not all institutions already have information security programs in place that are consistent with the Banking Agencies' Security Guidelines. In such cases, little or no modification to an institution's program will be required.'' *See* Banking Agencies' Security Guidelines, *supra* note 23. The statement was made in the analysis of whether the Guidelines would constitute ''a significant regulatory action'' for purposes of Executive Order 12866, which includes an action that would have an annual effect on the economy of $100 million or more or adversely affect in a material way the economy, a sector of the economy, productivity, competition, jobs, the environment, public health or safety, or State, local, or tribal governments or communities. The Board and the FDIC did not prepare an analysis under Executive Order 12866.

its existing safeguarding policies and procedures in compliance with the Banking Agencies' safeguarding guidance or the FTC's rules.

In addition to an institution's size, the adequacy of its safeguards, and its operations, we expect that institutions' information security programs would vary considerably depending on the way in which each collects information, the number and types of entities to which each transfers information, and the ways in which each stores, transfers, and disposes of personal information. Based on conversations with representatives of covered institutions and information collected from limited inquiries of institutions, our staff estimates that the additional initial costs that an institution could incur to comply with the proposed amendments could range from 0 to 10 percent of its current costs of maintaining an information security program. Our staff also estimates that the additional costs an institution could incur for ongoing compliance with the proposed amendments could range from 0 to 5 percent of its current costs.[158] For purposes of the PRA, staff estimates that for a smaller institution, the initial costs could range from between $500 and $100,000, with an approximate cost of $18,560 per smaller institution.[159] Staff also estimates that for a smaller institution, additional ongoing costs could range from between $250 and $50,000, with an approximate cost of $10,764 per smaller institution per year.[160] With respect to a larger institution, again for purposes of the PRA, staff estimates that initial costs could range from between $20,000 and $1 million, with an approximate cost of $172,732 per larger institution.[161] Staff further estimates that for a larger institution, additional ongoing costs could range from between $10,000 and $500,000 per year, with an approximate cost of $51,084 per larger institution per year.[162] We note that an institution that currently incurs the highest estimated costs for its information security program seems likely already to have a comprehensive information security program and therefore would be less likely to require program enhancements to comply with the rule. Accordingly, the high end of the range of estimated costs for institutions may be excessive.

We request comment on our estimated costs and our rationale underlying them, and any aspect of the estimates or other costs that we have not considered. We seek information about particular costs of compliance as well as information as to any overall percentage increase in costs that firms would likely incur as a result of the proposed amendments. We request comment accompanied with statistical or other quantitative information, and comment on the experiences of institutions in addressing the circumstances addressed above. Commenters should identify the metrics of any empirical data that support their cost estimates.

B. Costs and Benefits of Broadened Scope of Information and of Covered Institutions

The proposed rule amendments would broaden the scope of information covered by the safeguards and disposal rules. From the perspective of ease of compliance, we anticipate that institutions would benefit from having a common set of rules that apply to both nonpublic personal information about customers and consumer report information. We also expect that investors would benefit from expanding the scope of information covered by the safeguards and disposal rules because both terms exclude some information that without protections could more easily be used to obtain unauthorized access to investors' personal financial information. Because we expect that this expansion of the scope of information covered by the safeguards and disposal rules would not require modification of institutions' current policies and procedures, or their systems and databases for implementing these policies and procedures, and because many firms currently protect nonpublic personal information about customers and consumer report information in the same way, we expect that the proposal would result in no significant, if any, additional costs to institutions.

The amendments also would expand the scope of the safeguards rule to include registered transfer agents, limit the scope of the safeguards rule to exclude notice-registered broker-dealers, and extend the disposal rule to apply to natural persons. As noted above, bringing registered transfer agents within the scope of our safeguards rule should benefit investors because these institutions maintain sensitive personal information. We included registered transfer agents in our estimate of the costs of the proposed information security and security breach procedures above.[163] Because transfer agents are currently subject to the FTC Safeguards Rule, which, if the proposed amendments were adopted, would be substantially similar to the Commission's safeguards and disposal rules, we do not anticipate that there would be any unique or unusual costs to transfer agents, beyond those discussed above. Similarly, we do not anticipate any costs or benefits resulting from the proposal to exclude notice-registered broker-dealers from Regulation S–P because they would be subject to the CFTC's substantially similar safeguards rules. This proposal would simply clarify that notice-registered broker-dealers need not comply with both Regulation S–P and the CFTC's rules.

We expect that the proposal to include natural persons within the scope of the disposal rule would benefit investors by establishing a system designed to ensure that personal information is disposed of properly by employees, particularly those who may work in branches far from a covered institution's main office. We also believe that this proposal would benefit investors by requiring compliance by natural persons, associated with a covered institution, who are directly responsible for properly disposing of personal information consistent with the institution's policies. We do not expect that this proposal would result in costs to institutions beyond those that would be imposed by the more specific standards analyzed above in section V.A.2. Specifically, we believe that any changes that would be required to covered institutions' policies and procedures or training programs to make it clear that individuals (not just firms) would have responsibility for complying with the disposal rule are captured in our estimates above.

We request comment on these estimates of benefits and costs and our rationale underlying them, and any aspect of the estimates or other benefits or costs that we have not considered. In particular, we request comment accompanied with statistical or other quantitative evidence, and comment on the experiences of institutions in addressing the circumstances addressed above. Commenters should identify the metrics and sources of any empirical data that support their cost estimates.

C. Costs and Benefits of Maintaining Written Records

The proposed amendments would require covered institutions to maintain

[158] While we estimate that additional initial and ongoing costs would vary significantly across wide ranges, we estimate that the average cost per institution would be concentrated in the lower end of those ranges because, as noted, we believe that most institutions have already developed and adopted safeguarding and disposal polices and procedures, and are maintaining these policies and procedures, in accordance (or substantially in accordance) with the proposed rule amendments.

[159] *See supra* note 112 and accompanying text.

[160] *See supra* note 116 and accompanying text.

[161] *See supra* note 114 and accompanying text.

[162] *See supra* note 119 and accompanying text.

[163] *See supra* section V.A.2.

and preserve, in an easily accessible place, written records of the safeguards and disposal policies and procedures. The amendments also would require that institutions document compliance with their policies and procedures, and that records would have to be maintained for a period consistent with current requirements for similar records. We expect that this proposal would benefit investors by enabling the Commission's examination staff to evaluate whether institutions are in compliance with the requirements of the proposed amendments to the safeguards and disposal rules. We anticipate that institutions are unlikely to incur significant costs in maintaining records or documenting compliance to meet the requirements of this proposal because we would expect to establish a date for compliance with these amendments that would permit institutions to document and maintain these records in the normal course of ordinary business. Thus, we do not expect that this proposal would result in costs to institutions beyond those that would be imposed by the more specific standards analyzed above in section V.A.2.

We request comment on these estimates of benefits and costs and our rationale underlying them, and any aspect of the estimates or other benefits or costs that we have not considered. In particular, we request comment accompanied with statistical or other quantitative evidence, and comment on the experiences of institutions in addressing the circumstances addressed above. Commenters should identify the metrics and sources of any empirical data that support their cost estimates.

D. Costs and Benefits of Proposed New Exception

Our proposed amendments would create a new exception from Regulation S–P's notice and opt out requirements for disclosures of limited information in connection with the departure of a representative of a broker-dealer or investment adviser. The proposal should enhance information security by providing a clear framework for transferring limited information from one firm to another in this context. At firms that choose to rely on it, the proposed exception also should reduce potential incentives some representatives may have to take information with them secretly when they leave. In addition, the amendment should promote investor choice regarding whether to follow a departing representative to another firm. Institutions that choose to rely on the proposed exception also should benefit from the greater legal certainty that it would provide. We expect that institutions would incur minimal costs in retaining a written record of the information that would be disclosed in connection with a representative's departure, and expect that for a number of firms such costs are incurred already in the ordinary course of business.[164] Institutions need not provide these disclosures. Thus we anticipate that only those that expect the potential benefits from the disclosure would justify any associated costs would make the disclosures.

We request comment on this cost estimate and our rationale underlying it, and any aspect of the estimates or other costs that we have not considered. In particular, we request comment accompanied with statistical or other quantitative evidence, and the experiences of institutions in addressing the circumstances addressed above. Commenters should identify the metrics and sources of any empirical data that support their cost estimates.

E. Request for Comment

We request comment on all aspects of this cost-benefit analysis, including comment as to whether the estimates we have used in our analysis are reasonable. We welcome comment on any aspect of our analysis, the estimates we have made, and the assumptions we have described. In particular, we request comment as to any costs or benefits we may not have considered here that could result from the adoption of the proposed amendments. We also request comment on the numerical estimates we have made here, and request comment and specific costs and benefits from covered institutions that have experienced any of the situations analyzed above.

VI. Initial Regulatory Flexibility Analysis

This Initial Regulatory Flexibility Analysis (''IRFA'') has been prepared in accordance with 5 U.S.C. 603. It relates to proposed amendments to Regulation S–P that seek to strengthen the protections for safeguarding and disposing of sensitive personal information and provide a limited exception to notice and opt out requirements intended to augment investors' ability to choose whether to follow personnel who move from one broker-dealer or registered investment adviser to another. The proposed amendments would: (i) Require covered institutions to adopt more specific standards under the safeguards rule, including standards that would apply to security breach incidents; (ii) broaden the scope of information and the types of institutions and persons covered by the rules; and (iii) require covered institutions to maintain written records of the policies and procedures and their ongoing compliance with those polices and procedures. The proposed amendments also would require covered institutions seeking to rely on the new exception related to departing representatives to maintain a record of the information disclosed under the exception to a representative's new firm.

A. Reasons for the Proposed Action

We have become concerned with the significant increase in the number of information security breaches that have come to light in recent years and the potential created by such breaches for misuse of personal financial information, including identity theft. We are concerned that some firms do not regularly reevaluate and update their safeguarding programs to deal with increasingly sophisticated methods of attack. To help prevent and address security breaches at covered institutions, we propose to require more specific standards for safeguarding personal information, including standards for responding to data security breaches. In order to provide better protection against unauthorized disclosure of personal financial information, we believe that the scope of information covered by the current safeguards and disposal rules should be broader.

We also propose a new exception to Regulation S–P's notice and opt out requirements to permit limited disclosures of investor information when a registered representative of a broker-dealer or a supervised person of an investment adviser moves from one brokerage or advisory firm to another. The proposed exception should provide legal certainty to firms that choose to rely on it and reduce incentives some representatives may have to take information with them secretly when they leave. We believe this amendment also would help to augment investors' ability to choose whether or not to follow a departing representative to another firm.

B. Objectives of the Proposed Action

The overall objectives of the proposed amendments are to: (i) Strengthen the protections for safeguarding and disposing of sensitive personal information; and (ii) provide a limited exception to Regulation S–P's notice and opt out requirements that would preserve investors' ability to choose whether to follow personnel who move

[164] *See supra* note 91 and accompanying text.

from one broker-dealer or investment adviser to another. We believe that the proposed amendments would help to:

- Prevent and mitigate information security breach incidents;
- Ensure that sensitive financial information is not disposed of improperly;
- Ensure that firms regularly review and update their safeguarding policies and procedures;
- Ensure that the full range of appropriate information and all relevant types of institutions regulated by the Commission are covered by Regulation S–P's requirements; and
- Enhance information security at firms choosing to rely on a new exemption for disclosures of limited information when representatives move from one firm to another by providing a clear framework for such disclosures and promote investor choice regarding whether or not to follow a departing representative to another firm.

C. Legal Basis

The amendments to Regulation S–P are proposed pursuant to the authority set forth in Sections 501, 504, 505, and 525 of the GLBA, Section 628(a)(1) of the FCRA, Sections 17, 17A, 23, and 36 of the Exchange Act, Sections 31(a) and 38 of the Investment Company Act, and Sections 204 and 211 of the Investment Advisers Act.[165]

D. Small Entities Subject to the Proposed Rule Amendments

The proposed amendments to Regulation S–P would affect brokers, dealers, registered investment advisers, investment companies, and registered transfer agents, including entities that are considered to be a small business or small organization (collectively, ''small entity'') for purposes of the Regulatory Flexibility Act. For purposes of the Regulatory Flexibility Act, under the Exchange Act a broker or dealer is a small entity if it: (i) Had total capital of less than $500,000 on the date in its prior fiscal year as of which its audited financial statements were prepared or, if not required to file audited financial statements, on the last business day of its prior fiscal year; and (ii) is not affiliated with any person that is not a small entity.[166] A registered transfer agent is a small entity if it: (i) Received less than 500 items for transfer and less than 500 items for processing during the preceding six months; (ii) transferred items only of issuers that are small entities; (iii) maintained master shareholder files that in the aggregate contained less than 1,000 shareholder accounts or was the named transfer agent for less than 1,000 shareholder accounts at all times during the preceding fiscal year; and (iv) is not affiliated with any person that is not a small entity.[167] Under the Investment Company Act, investment companies are considered small entities if they, together with other funds in the same group of related funds, have net assets of $50 million or less as of the end of its most recent fiscal year.[168] Under the Investment Advisers Act, a small entity is an investment adviser that: (i) Manages less than $25 million in assets; (ii) has total assets of less than $5 million on the last day of its most recent fiscal year; and (iii) does not control, is not controlled by, and is not under common control with another investment adviser that manages $25 million or more in assets, or any person that has had total assets of $5 million or more on the last day of the most recent fiscal year.[169]

Based on Commission filings, we estimate that 894 broker-dealers, 153 registered transfer agents, 203 investment companies, and 760 registered investment advisers may be considered small entities.

E. Reporting, Recordkeeping, and Other Compliance Requirements

The proposed amendments to Regulation S–P would require more specific compliance requirements and create new reporting requirements for institutions that experience a breach of information security. The proposed amendments also would introduce new mandatory recordkeeping requirements.

Under the proposed amendments to Regulation S–P, covered institutions would have to develop, implement, and maintain a comprehensive ''information security program'' for protecting personal information and responding to unauthorized access to or use of personal information. We expect that some covered institutions, including covered institutions that are small entities, would be required to supplement their current costs by the costs involved in reviewing and, as appropriate, revising their current safeguarding policies and procedures, including their data security breach response procedures and disposal rule procedures, to comply with the more specific requirements of the proposed amendments. Initially this would require institutions to: (i) Designate an employee or employees as coordinator for their information security program; (ii) identify in writing reasonably foreseeable security risks that could result in the unauthorized or compromise of personal information or personal information systems; (iii) create a written record of their design and implementation of their safeguards to control identified risks; (iv) train staff to implement their information security program; and (v) oversee service providers and document that oversight in writing.

Institutions also would have to review existing safeguarding procedures relating to data security breach incidents. This would include: (i) Assessing current policies and procedures for responding to data breach incidents; and (ii) designing and implementing written policies and procedures to assess, control, and investigate incidents of unauthorized access or use of sensitive personal information, as well as policies and procedures for, under certain conditions, notifying individuals and the Commission or, in the case of a broker-dealer, the appropriate designated examining authority.

To comply with these amendments on an ongoing basis, institutions would have to implement procedures to: (i) Regularly test or monitor, and maintain a written record of the effectiveness of their safeguards' key controls, systems and procedures (including access controls, controls related to data security breach incidents, and controls related to employee training and supervision); (ii) augment staff training as necessary; (iii) provide continued oversight of service providers; and (iv) regularly evaluate and adjust their information security program in light of their regular testing and monitoring, changes in technology, their business operations or arrangements, and other material circumstances.

Institutions also would have to respond appropriately to incidents of data security breach as may occur on an ongoing basis. This would include following their written procedures to: (i) Assess the nature and scope of the incident; (ii) take appropriate steps to contain and control the incident; (iii) promptly conduct a reasonable investigation and make a written determination of the likelihood that sensitive personal information has been or will be misused; (iv) if misuse of information has occurred or is reasonably likely, notify affected individuals as soon as possible; and (v) if an individual identified with the information has suffered substantial

[165] 15 U.S.C. 6801, 6804, 6805, and 6825; 15 U.S.C. 1681w(a)(1); 15 U.S.C. 78q, 78q–1, 78w, and 78mm; 15 U.S.C. 80a–30(a), 80a–37; and 15 U.S.C. 80b–4, 80b–11.

[166] 17 CFR 240.0–10.

[167] *Id.*

[168] 17 CFR 270.0–10.

[169] 17 CFR 275.0–7.

harm or inconvenience, or any unauthorized person has intentionally obtained access to or used sensitive personal information, notify the Commission or an appropriate designated examining authority as soon as possible on proposed Form SP–30.

Overall, we expect there would be incremental costs associated with the proposed amendments to Regulation S–P. Some proportion of large or small institutions would be likely to experience some increase in costs to comply with the proposed amendments if they are adopted.

More specifically, we estimate that with respect to the more specific safeguarding elements, covered institutions would incur one-time costs that could include the costs of assessment and revision of safeguarding standards, staff training, and reviewing and entering into contracts with service providers.[170] We also estimate that the ongoing, long-term costs associated with the proposed amendments could include costs of regularly testing or monitoring the safeguards, augmenting staff training, providing continued oversight of service providers, evaluating and adjusting safeguards, and responding appropriately to incidents of data security breach.[171]

We encourage written comments regarding this analysis. We solicit comments as to whether the proposed amendments could have an effect that we have not considered. We also request that commenters describe the nature of any impact on small entities and provide empirical data to support the extent of the impact.

F. Duplicative, Overlapping, or Conflicting Federal Rules

As discussed above, the proposed amendments would impose requirements that covered institutions maintain and document a written information security program. The proposed amendments also would require reporting to individuals and appropriate regulators after certain serious data breach incidents. Covered institutions are subject to requirements elsewhere under the federal securities laws and rules of the self-regulatory organizations that require them to adopt written policies and procedures that may relate to some similar issues.[172] The proposed amendments to Regulation S–P, however, would not require covered institutions to maintain duplicate copies of records covered by the rule, and an institution's information security program would not have to be maintained in a single location. Moreover, although the proposed amendments would require covered institutions to keep certain records that may be required under existing recordkeeping rules, the purposes of the requirements are different, and institutions need not maintain duplicates of the records themselves.[173] We believe, therefore, that any duplication of regulatory requirements would be limited and would not impose significant additional costs on covered institutions including small entities. We believe there are no other federal rules that duplicate, overlap, or conflict with the proposed reporting requirements.

G. Significant Alternatives

The Regulatory Flexibility Act directs us to consider significant alternatives that would accomplish the stated objectives, while minimizing any significant adverse impact on small entities. In connection with the proposed amendments, we considered the following alternatives:

(i) Establishing different compliance or reporting standards that take into account the resources available to small entities;

(ii) The clarification, consolidation, or simplification of the reporting and compliance requirements under the rule for small entities;

(iii) Use of performance rather than design standards; and

(iv) Exempting small entities from coverage of the rule, or any part of the rule.

With regard to the first alternative, we have proposed amendments to Regulation S–P that would continue to permit institutions substantial flexibility to design safeguarding policies and procedures appropriate for their size and complexity, the nature and scope of their activities, and the sensitivity of the personal information at issue. We nevertheless believe it necessary to provide a more specific framework of elements that every institution should consider and address, regardless of its size. The proposed amendments to Regulation S–P arise from our concern with the increasing number of information security breaches that have come to light in recent years, particularly those involving institutions regulated by the Commission. Establishing different compliance or reporting requirements for small entities could lead to less favorable protections for these entities' customers and compromise the effectiveness of the proposed amendments.

With regard to the second alternative, we believe that the proposed amendments should, by their operation, simplify reporting and compliance requirements for small entities. Small covered institutions are likely to maintain personal information on fewer individuals than large covered institutions, and they are likely to have relatively simple personal information systems. Under proposed paragraph (a)(1) of Section 30, the information security programs that would be required by the proposed amendments would have to be appropriate to a covered institution's size and complexity, and the nature and scope of its activities. Accordingly, we believe that the requirements of the proposed amendment already would be simplified for small entities. We also believe that the requirements of the proposed amendments could not be further simplified, or clarified or consolidated, without compromising the investor protection objectives the proposed amendments are designed to achieve.

With regard to the third alternative, the proposed amendments are for the most part performance based. Rather than specifying the types of policies and procedures or the technologies that an institution would be required to use to safeguard personal information, the proposed amendments would require the institution to assess the types of risks that it is likely to face and to address those in the manner the institution believes most appropriate. With respect to the specific requirements regarding notifications in the event of a data security breach, we have proposed that institutions provide only the information that seems most relevant for the Commission, a self-regulatory organization, or a consumer to know in order to adequately assess the potential damage that could result from the breach and to develop an appropriate response.

Finally, with regard to alternative four, we believe that an exemption for small entities would not be appropriate.

---

[170] *See supra* section IV.A.3.

[171] *Id.*

[172] *See, e.g.*, 15 U.S.C. 80b–4a (requiring each adviser registered with the Commission to have written policies and procedures reasonably designed to prevent misuse of material non-public information by the adviser or persons associated with the adviser); and NASD Rule 3010 (requiring each broker-dealer to establish and maintain written procedures to supervise the types of business it is engaged in and to supervise the activities of registered representatives and associated persons, which could include registered investment advisers).

[173] *See, e.g.*, 17 CFR 240.17a–3 (requiring broker-dealers to make and keep, among other things, blotters or other records of original entry, securities position records, and order tickets) and 17 CFR 270.31a–1(b)(11) (requiring investment companies to maintain, among other things, minute books of directors' meetings and ''files of all advisory material received from the investment adviser'').

Small entities are as vulnerable as large ones to the types of data security breach incidents we are trying to address. We believe that the specific elements we have proposed must be considered and incorporated into the policies and procedures of all covered institutions, regardless of their size, to mitigate the potential for fraud or other substantial harm or inconvenience to investors. Exempting small entities from coverage of the proposed amendments or any part of the proposed amendments could compromise the effectiveness of the proposed amendments and harm investors by lowering standards for safeguarding investor information maintained by small covered institutions. Excluding small entities from requirements that would be applicable to larger covered institutions also could create competitive disparities between large and small entities, for example by undermining investor confidence in the security of information maintained by small covered institutions.

We request comment on whether it is feasible or necessary for small entities to have special requirements or timetables for, or exemptions from, compliance with the proposed amendments. In particular, could any of the proposed amendments be altered in order to ease the regulatory burden on small entities, without sacrificing the effectiveness of the proposed amendments?

H. Request for Comments

We encourage the submission of comments with respect to any aspect of this IRFA. In particular, we request comments regarding: (i) The number of small entities that may be affected by the proposed amendments; (ii) the existence or nature of the potential impact of the proposed amendments on small entities discussed in the analysis; and (iii) how to quantify the impact of the proposed amendments. Commenters are asked to describe the nature of any impact and provide empirical data supporting the extent of the impact. Such comments will be considered in the preparation of the Final Regulatory Flexibility Analysis, if the proposed amendments are adopted, and will be placed in the same public file as comments on the proposed amendments. Comments should be submitted to the Commission at the addresses previously indicated.

VII. Consideration of Burden on Competition and Promotion of Efficiency, Competition and Capital Formation

Exchange Act Section 23(a)(2) requires us, when adopting rules under the Exchange Act, to consider the impact any new rule would have on competition.[174] In addition, Section 23(a)(2) prohibits us from adopting any rule that would impose a burden on competition not necessary or appropriate in furtherance of the purposes of Title I of the Exchange Act. The proposed amendments to Regulation S–P would: (i) Require more specific standards under the safeguards rule, including standards that would apply to data security breach incidents; (ii) broaden the scope of information and the types of institutions and persons covered by the safeguards and disposal rules; and (iii) require covered institutions to maintain written records of their policies and procedures and their compliance with those policies and procedures. The proposed amendments also would create a new exception from Regulation S–P's notice and opt-out requirements for firms to transfer limited investor information regarding clients of departing representatives to those representatives' new firms.

Other financial institutions are currently subject to substantially similar safeguarding and data breach response requirements under rules adopted by the Banking Agencies and the FTC. Under the proposed amendments, all financial institutions would have to bear similar costs in implementing substantially similar rules thus enhancing competition. We expect that the proposed amendment to create the new exception for firms to transfer limited investor information regarding clients of departing representatives to those representatives' new firms would not limit and might promote competition in the securities industry by providing legal certainty for firms that choose to rely on it and by facilitating the transition for customers who choose to follow a departing representative to a new firm.

In addition, Exchange Act Section 3(f), Investment Company Act Section 2(c), and Investment Advisers Act Section 202(c) require us, when engaging in rulemaking where we are required to consider or determine whether an action is necessary or appropriate in the public interest, to consider, in addition to the protection of investors, whether the action will promote efficiency, competition, and capital formation.[175] Our analysis on competition is discussed above. As discussed above, the proposed amendments could result in additional costs for covered institutions, which could affect the efficiency of these institutions. On the other hand, the amendments could promote investor confidence and bring new investors to these institutions. In the long term, the proposed amendments also could help reduce covered institutions' costs by mitigating the frequency and consequences of information security breaches. We do not believe the proposed amendments would have a significant effect on capital formation, although if the proposals lead to better information security practices at covered institutions, potential investors could feel more comfortable investing money in the capital markets. As a result, we expect that the potential additional expense of compliance with these proposed rule amendments would have little, if any, adverse effect on efficiency, competition, and capital formation.

We request comment as to whether our estimates of the burdens the proposed amendments would have on covered institutions are reasonable. We welcome comment on any aspect of this analysis, and specifically request comment on any effect the proposed amendments might have on the promotion of efficiency, competition, and capital formation that we have not considered. Would the proposed amendments or their resulting costs affect the efficiency, competition, and capital formation of covered institutions and their businesses? Commenters are requested to provide empirical data and other factual support for their views to the extent possible.

VIII. Small Business Regulatory Enforcement Fairness Act

For purposes of the Small Business Regulatory Enforcement Fairness Act of 1996, or ''SBREFA,'' [176] we must advise OMB as to whether the proposed regulation constitutes a ''major'' rule. Under SBREFA, a rule is considered ''major'' if, upon adoption, it results or is likely to result in:

- An annual effect on the economy of $100 million or more (either in the form of an increase or a decrease);
- A major increase in costs or prices for consumers or individual industries; or
- Significant adverse effect on competition, investment or innovation.

If a rule is ''major,'' its effectiveness will generally be delayed for 60 days pending Congressional review. We

[174] 15 U.S.C. 78w(a)(2).

[175] 15 U.S.C. 78c(f); 15 U.S.C. 80a–2(c); and 15 U.S.C. 80b–2(c).

[176] Pub. L. No. 104–121, Title II, 110 Stat. 857 (1996) (codified in various sections of titles 5 and 15 of the United States Code, and as a note to 5 U.S.C. 601).

request comment on the potential impact of the proposed regulation on the economy on an annual basis. Commenters are requested to provide empirical data and other factual support for their view to the extent possible.

IX. Statutory Authority

The Commission is proposing to amend Regulation S–P pursuant to authority set forth in Sections 501, 504, 505 and 525 of the GLBA (15 U.S.C. 6801, 6804, 6805 and 6825), Section 628(a)(1) of the FCRA (15 U.S.C. 1681w(a)(1)), Sections 17, 17A, 23, and 36 of the Exchange Act (15 U.S.C. 78q, 78q–1, 78w, and 78mm), Sections 31(a) and 38 of the Investment Company Act (15 U.S.C. 80a–30(a) and 80a–37), and Sections 204 and 211 of the Investment Advisers Act (15 U.S.C. 80b–4 and 80b–11).

X. Text of Proposed Rules and Rule Amendments

List of Subjects in 17 CFR Part 248

Brokers, Dealers, Investment advisers, Investment companies, Privacy, Reporting and recordkeeping requirements, Transfer agents.

For the reasons set out in the preamble, the Commission proposes to amend 17 CFR part 248 as follows.

1. Revise the heading of part 248 to read as follows:

PART 248—REGULATION S–P: PRIVACY OF CONSUMER FINANCIAL INFORMATION AND SAFEGUARDING PERSONAL INFORMATION

2. Revise the authority citation for part 248 to read as follows:

Authority: 15 U.S.C. 78q, 78q–1, 78w, 78mm, 80a–30(a), 80a–37, 80b–4, 80b–11, 1681w(a)(1), 6801–6809, and 6825.

3. Section 248.1(b) is amended by removing ''(b)'' from the reference to ''§ 248.30(b)'' in the first sentence of the paragraph.

4. Section 248.2(b) is amended by removing ''(b)'' from the reference to ''§ 248.30(b)'' in the first sentence.

5. Section 248.3(u) is amended by:

a. Removing ''or'' at the end of paragraph (u)(1)(ii);

b. Removing the period at the end of paragraph (u)(1)(iii) and in its place adding ''; or''; and

d. Adding paragraph (u)(1)(iv) to read as follows:

§ 248.3 Definitions.

* * * * *

(u) * * *

(1) * * *

(iv) Handled or maintained by you or on your behalf that is identified with any consumer, or with any employee, investor, or securityholder who is a natural person.

* * * * *

6. Remove the heading of subpart A of part 248 and add in its place the following undesignated center heading: ''Privacy and Opt Out Notices''.

7. Remove the heading of subpart B of part 248 and add in its place the following undesignated center heading: ''Limits on Disclosures''.

8. Remove the heading of subpart C of part 248 and add in its place the following undesignated center heading: ''Exceptions''.

9. Section 248.15 is amended by:

a. Removing the word ''or'' at the end of paragraph (a)(6);

b. Removing the period at the end of paragraph (a)(7)(iii) and in its place adding ''; or''; and

c. Adding paragraph (a)(8).

The addition reads as follows:

§ 248.15 Other exceptions to notice and opt out requirements.

(a) * * *

(8) To a broker, dealer, or investment adviser registered with the Commission in order to allow one of your representatives who leaves you to become the representative of another broker, dealer, or registered investment adviser to solicit customers to whom the representative personally provided a financial product or service on your behalf, provided:

(i) The information is limited to a customer's name, a general description of the type of account and products held by the customer, and the customer's contact information, including the customer's address, telephone number, and email information;

(ii) The information does not include any customer's account number, Social Security number, or securities positions; and

(iii) You require your departing representative to provide to you, not later than the representative's separation from employment with you, a written record of the information that will be disclosed pursuant to this exception, and you maintain and preserve such records under § 248.30(c).

(iv) For purposes of this section, representative means:

(A) A natural person associated with a broker or dealer registered with the Commission, who is registered or approved in compliance with § 240.15b7–1 of this chapter; or

(B) A supervised person of an investment adviser as defined in section 202(a)(25) of the Investment Advisers Act of 1940 (15 U.S.C. 80b–2(a)(25)).

10. Remove the heading of subpart D of part 248 and add in its place the following undesignated center heading: ''Relation to Other Laws; Effective Date''.

11. Amend part 248 by adding the undesignated center heading, ''Information Security Programs'' before § 248.30, and revising § 248.30 to read as follows:

INFORMATION SECURITY PROGRAMS

§ 248.30 Information security programs for personal information; records of compliance.

(a) *Information security programs.*—(1) *General requirements.* Every broker or dealer other than a notice-registered broker or dealer, every investment company, and every investment adviser or transfer agent registered with the Commission, must develop, implement, and maintain a comprehensive information security program. Your program must include written policies and procedures that provide administrative, technical, and physical safeguards for protecting personal information, and for responding to unauthorized access to or use of personal information. Your program also must be appropriate to your size and complexity, the nature and scope of your activities, and the sensitivity of any personal information at issue.

(2) *Objectives.* Your information security program must be reasonably designed to:

(i) Ensure the security and confidentiality of personal information;

(ii) Protect against any anticipated threats or hazards to the security or integrity of personal information; and

(iii) Protect against unauthorized access to or use of personal information that could result in substantial harm or inconvenience to any consumer, employee, investor or securityholder who is a natural person.

(3) *Safeguards.* In order to develop, implement, and maintain your information security program, you must:

(i) Designate in writing an employee or employees to coordinate your information security program;

(ii) Identify in writing reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of personal information and personal information systems that could result in the unauthorized disclosure, misuse, alteration, destruction or other compromise of such information or systems;

(iii) Design and implement safeguards to control the risks you identify, and maintain a written record of your design;

(iv) Regularly test or otherwise monitor, and maintain a written record

of the effectiveness of the safeguards' key controls, systems, and procedures, including the effectiveness of:

(A) Access controls on personal information systems;

(B) Controls to detect, prevent and respond to incidents of unauthorized access to or use of personal information; and

(C) Employee training and supervision relating to your information security program.

(v) Train staff to implement your information security program;

(vi) Oversee service providers, and document in writing that in your oversight you are:

(A) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the personal information at issue; and

(B) Requiring your service providers by contract to implement and maintain appropriate safeguards; and

(vii) Evaluate and adjust your information security program accordingly in light of:

(A) The results of the testing and monitoring required by paragraph (a)(3)(iv) of this section;

(B) Relevant changes in technology;

(C) Any material changes to your operations or business arrangements; and

(D) Any other circumstances that you know or reasonably believe may have a material impact on your information security program.

(4) *Procedures for responding to unauthorized access or use.* At a minimum, your information security program must include written procedures to:

(i) Assess the nature and scope of any incident involving unauthorized access to or use of personal information, and maintain a written record of the personal information systems and types of personal information that may have been accessed or misused;

(ii) Take appropriate steps to contain and control the incident to prevent further unauthorized access to or use of personal information and maintain a written record of the steps you take;

(iii) After becoming aware of an incident of unauthorized access to sensitive personal information, promptly conduct a reasonable investigation, determine the likelihood that the information has been or will be misused, and maintain a written record of your determination;

(iv) If you determine that misuse of the information has occurred or is reasonably possible, notify each individual with whom the information is identified as soon as possible in accordance with paragraph (a)(5) of this section and maintain a written record that you provided notification; provided however that if an appropriate law enforcement agency determines that notification will interfere with a criminal investigation and requests in writing that you delay notification, you may delay notification until it no longer interferes with the criminal investigation; and

(v) If you are a broker or dealer other than a notice-registered broker or dealer, provide written notice on Form SP–30 to your designated examining authority (*see* 17 CFR 240.17d–1), and, if you are an investment company or an investment adviser or transfer agent registered with the Commission, provide written notice on Form SP–30 to the principal office of the Commission, as soon as possible after you become aware of any incident of unauthorized access to or use of personal information in which:

(A) There is a significant risk that an individual identified with the information might suffer substantial harm or inconvenience; or

(B) An unauthorized person has intentionally obtained access to or used sensitive personal information.

(5) *Notifying individuals of unauthorized access or use.* If you determine that an unauthorized person has obtained access to or used sensitive personal information, and you determine that misuse of the information has occurred or is reasonably possible, you must notify each individual with whom the information is identified in a clear and conspicuous manner and by a means designed to ensure that the individual can reasonably be expected to receive it. The notice must:

(i) Describe in general terms the incident and the type of sensitive personal information that was the subject of unauthorized access or use;

(ii) Describe what you have done to protect the individual's information from further unauthorized access or use;

(iii) Include a toll-free telephone number to call, or if you do not have any toll-free number, include a telephone number to call and the address and the name of a specific office to write for further information and assistance;

(iv) If the individual has an account with you, recommend that the individual review account statements and immediately report any suspicious activity to you; and

(v) Include information about the availability of online guidance from the FTC regarding steps an individual can take to protect against identity theft, a statement encouraging the individual to report any incidents of identity theft to the FTC, and the FTC's Web site address and toll-free telephone number that individuals may use to obtain the identity theft guidance and report suspected incidents of identity theft.

(b) *Disposal of personal information.*—(1) *Standard.* Every broker or dealer other than a notice-registered broker or dealer, every investment company, every investment adviser or transfer agent registered with the Commission, and every natural person who is an associated person of a broker or dealer, a supervised person of an investment adviser registered with the Commission, or an associated person of a transfer agent registered with the Commission, that maintains or otherwise possesses personal information for a business purpose must properly dispose of the information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

(2) *Written policies, procedures and records.* Every broker or dealer, other than a notice-registered broker or dealer, every investment company, and every investment adviser and transfer agent registered with the Commission must:

(i) Adopt written policies and procedures that address the proper disposal of personal information according to the requirements of paragraph (b)(1) of this section; and

(ii) Document in writing its proper disposal of personal information in compliance with paragraph (b)(1) of this section.

(3) *Relation to other laws.* Nothing in this paragraph (b) shall be construed:

(i) To require any broker, dealer, investment company, investment adviser, transfer agent, associated person of a broker or dealer, supervised person of an investment adviser, or associated person of a transfer agent, to maintain or destroy any record pertaining to an individual that is not imposed under other law; or

(ii) To alter or affect any requirement imposed under any other provision of law to maintain or destroy records.

(c) *Recordkeeping.* (1) Every broker or dealer other than a notice-registered broker or dealer, every investment company, and every investment adviser or transfer agent registered with the Commission, must make and maintain the records and written policies and procedures required under paragraphs (a) and (b)(2) of this section. Every broker or dealer other than a notice-registered broker or dealer, and every investment adviser registered with the Commission seeking to rely on the

exception in § 248.15(a)(8) must make and maintain the records required by § 248.15(a)(8)(iii).

(2) Starting from when the record was made, or from when the written policy or procedure was last modified, the records and written policies and procedures required under paragraphs (a) and (b)(2) of this section, and the records made pursuant to § 248.15(a)(8)(iii), must be preserved in accordance with:

(i) 17 CFR 240.17a–4(b) by a broker or dealer other than a notice-registered broker or dealer;

(ii) 240.17Ad–7(b) by a transfer agent registered with the Commission;

(iii) 270.31a–2(a)(4)–(6) by an investment company; and

(iv) 275.204–2(e)(1) by an investment adviser registered with the Commission.

(d) *Definitions.* As used in this § 248.30, unless the context otherwise requires:

(1) *Associated person of a broker or dealer* has the same meaning as in section 3(a)(18) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(18)).

(2) *Associated person of a transfer agent* has the same meaning as in section 3(a)(49) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(49)).

(3) *Consumer report* has the same meaning as in section 603(d) of the Fair Credit Reporting Act (15 U.S.C. 1681a(d)).

(4) *Consumer report information* means any record about an individual, whether in paper, electronic or other form, that is a consumer report or is derived from a consumer report. Consumer report information also means a compilation of such records. Consumer report information does not include information that does not identify individuals, such as aggregate information or blind data.

(5) *Disposal* means:

(i) The discarding or abandonment of personal information; or

(ii) The sale, donation, or transfer of any medium, including computer equipment, on which personal information is stored.

(6) *Information security program* means the administrative, technical, or physical safeguards you use to access, collect, distribute, process, protect, store, use, transmit, dispose of, or otherwise handle personal information.

(7) *Notice-registered broker or dealer* means a broker or dealer registered by notice with the Commission under section 15(b)(11) of the Securities Exchange Act of 1934 (15 U.S.C. 78o(b)(11)).

(8) *Personal information* means any record containing consumer report information, or nonpublic personal information as defined in § 248.3(t), that is identified with any consumer, or with any employee, investor, or securityholder who is a natural person, whether in paper, electronic, or other form, that is handled or maintained by you or on your behalf.

(9) *Personal information system* means any method used to access, collect, store, use, transmit, protect, or dispose of personal information.

(10) *Sensitive personal information* means 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:

(i) Social Security number; or

(ii) Name, telephone number, street address, e-mail address, or online user name, in combination with the individual's account number, credit or debit card number, driver's license number, credit card expiration date or security code, mother's maiden name, password, personal identification number, biometric record, or other authenticating information.

(11) *Service provider* means any person or entity that receives, maintains, processes, or otherwise is permitted access to personal information through its provision of services directly to a broker, dealer, investment company, or investment adviser or transfer agent registered with the Commission.

(12) (i) *Substantial harm or inconvenience* means personal injury, or more than trivial financial loss, expenditure of effort or loss of time, including theft, fraud, harassment, impersonation, intimidation, damaged reputation, impaired eligibility for credit, or the unauthorized use of information identified with an individual to obtain a financial product or service, or to access, log into, effect a transaction in, or otherwise use the individual's account.

(ii) Substantial harm or inconvenience does not include unintentional access to personal information by an unauthorized person that results only in trivial financial loss, expenditure of effort or loss of time, such as if use of the information results only in your deciding to change the individual's account number or password.

(13) *Supervised person of an investment adviser* has the same meaning as in section 202(a)(25) of the Investment Advisers Act of 1940 (15 U.S.C. 80b–2(a)(25)).

(14) *Transfer agent* has the same meaning as in section 3(a)(25) of the Securities Exchange Act of 1934 (15 U.S.C. 78c(a)(25)).

12. Redesignate Appendix A to part 248 as Appendix B to part 248, and revise its heading to read as follows:

Appendix B to part 248—Sample Clauses

13. Add new Appendix A to part 248 to read as follows:

Appendix A to Part 248—Forms

(1) *Availability of Forms.* Any person may obtain a copy of Form S–P or Form SP–30 prescribed for use in this part by written request to the Securities and Exchange Commission, 100 F Street, NE., Washington, DC 20549. Any person also may view the forms on the Commission Web site as follows:

(a) Form S–P at: [Web site URL];

(b) Form SP–30 at: [Web site URL].

(2) *Form S–P.* Use of Form S–P by brokers, dealers, and investment companies, and by investment advisers registered with the Commission, constitutes compliance with the notice content requirements of §§ 248.6 and 248.7.

(3) *Form SP–30.* Form SP–30 must be used pursuant to § 248.30(a)(4)(v) as the notice of an incident of unauthorized access to or use of personal information to be filed with the appropriate designated examining authority by brokers or dealers other than notice-registered brokers or dealers, and to be filed with the Commission by investment companies, and by investment advisers and transfer agents registered with the Commission.

14. Add Form SP–30 (referenced in paragraph (3) of Appendix A to part 248) to read as follows:

Note: The text of Form SP–30 does not, and this amendment will not, appear in the Code of Federal Regulations.

UNITED STATES SECURITIES AND EXCHANGE COMMISSION

Washington, DC 20549

FORM SP–30

SECURITY INCIDENT REPORTING FORM

(Pursuant to § 248.30(a)(4)(v) of Regulation S–P (17 CFR 248.30(a)(4)(v)))

1. Provide identifying information (IARD/CRD number, CIK,* business name, principal business and mailing addresses, and telephone number).

* CIK stands for ''Central Index Key,'' which is the unique number the Commission assigns to each entity that submits filings to it.

2. Provide contact employee (name, title, address, and telephone number).

3. Type of Institution:

____Broker-Dealer
____Investment Adviser
____Investment Adviser/Broker-Dealer (Dual Registrant)
____Investment Company
____Transfer Agent

4. Describe the security incident (*e.g.*, unauthorized use of your customers' online trading accounts, unauthorized use of your employee's password to access sensitive personal information maintained on one of your databases, or unauthorized access to your files on an investment company's shareholders):

(a) Provide the date(s) of the incident;

(b) List Registrant's offices, divisions or branches involved;

(c) Describe personal information system(s) compromised;

(d) Describe the incident and identify anyone you reasonably believe accessed or used personal information without authorization or compromised the personal information system(s).

5. Provide information on third-party service provider(s) involved:

(a) Identify any third-party service provider involved;

(b) Describe the services provided;

(c) If the service provider is an affiliate, describe the affiliation;

(d) Describe the involvement of the service provider(s) in the incident.

6. Describe steps taken or that you plan to take to assess the incident.

7. Provide the number of individuals whose information appears to have been compromised:_____

8. Describe steps you have taken or plan to take to prevent improper use of any personal information that was or may be compromised by the incident.

9. Do you intend to notify affected individuals?

(a) If yes, when?

(b) If no, why not?

10. Describe any steps you have taken or any plan to review your policies and procedures in light of this incident.

11. Describe Customer account losses (to the extent known).

(a) Number of Customer Accounts Accessed: _____

(b) Unauthorized Money Transfers

(i) Initial Customer Losses from Actual or Attempted Unauthorized Transfers: $_____

(ii) Mitigation of Customer Losses from Firm's Efforts

(A) Surveillance/Investigative Intervention: $_____

(B) Recoveries from Receiving Parties: $_____

(C) Firm Compensation to Customers: $_____

(iii) Net Customer Losses: $_____

(c) Unauthorized Changes to Securities Portfolio (*e.g.*, Pump and Dump Schemes)

(i) Initial Customer Losses from Actual or Attempted Unauthorized Trading

(A) Value of Accounts Before the Unauthorized Trading: $_____

(B) Value of Accounts After the Unauthorized Trading: $_____

(C) Initial Customer Losses/Gains: $_____

(ii) Did the firm return the affected customer accounts to their positions before the unauthorized trading? Yes/No

(iii) Net Customer Losses/Gains: $_____

Dated: March 4, 2008.

By the Commission.

Nancy M. Morris,

Secretary.

[FR Doc. E8–4612 Filed 3–12–08; 8:45 am]

BILLING CODE 8011–01–P