INVESTMENT COMPANY INSTITUTE

1401 H Street, NW, Washington, DC 20005-2148, USA
202/326-5800 www.ici.org

May 2, 2008

Ms. Nancy M. Morris
Secretary
U.S. Securities and Exchange Commission
100 F Street, NE
Washington, DC 20549-9303

Re: Proposed Amendments to Regulation S-P
SEC File No. S7-06-08

Dear Ms. Morris:

The Investment Company Institute[1] supports the Securities and Exchange Commission replacing its existing data security rule in Regulation S-P with a more detailed and robust rule requiring registrants to have information security programs.[2] We additionally support patterning of the rule after similar rules adopted by the Department of the Treasury, the Federal Reserve System, and other Federal regulators of financial institutions because it will facilitate compliance by our members that are also subject to such regulators' jurisdiction. The other regulators' rules were adopted almost eight years ago and financial institutions are familiar with them and their operation.

While the Institute supports adoption of a more robust data security rule, we recommend several revisions to the Commission's proposal to facilitate compliance and better align its requirements with its intent and the provisions in the Gramm-Leach-Bliley Act (the "GLB Act") that address the protection of customers' non-public personal information. In particular, we recommend that the Commission:

---

[1] The Investment Company Institute is the national association of U.S. investment companies, including mutual funds, closed-end funds, exchange-traded funds (ETFs), and unit investment trusts (UITs). ICI seeks to encourage adherence to high ethical standards, promote public understanding, and otherwise advance the interests of funds, their shareholders, directors, and advisers. Members of ICI manage total assets of $12.31 trillion and serve almost 90 million shareholders.

[2] *See Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information,* Release Nos. 34-57427 and IA-2712, 73 FED. REG. 13692 (Mar. 13, 2008) (the "Release").

- Permit registrants to assign responsibility for the program's implementation to either a position that is charged with being the information security program coordinator or to a named individual;
- Clarify the rule's testing requirements;
- Provide greater clarity regarding issues involving unauthorized access triggering breach notices;
- Clarify and conform the breach notice standards used for individuals to those applicable to informing the Commission of a breach on Form SP-30;
- Revise the content and filing requirements for Form SP-30;
- Clarify the party responsible for providing notice of unauthorized access and filing Form SP-30;
- Conform the data subject to the rule to that subject to the Commission's rulemaking authority under the GLB Act;
- Provide a sufficient compliance period; and
- Require the Commission and each registered self-regulatory organization to have an information security program similar to that proposed in Reg. S-P.

Each of these recommendations is discussed in detail below.

I. THE RULE'S PROPOSED SAFEGUARDS

As proposed, Rule 248.30 would require every broker-dealer, investment company, investment adviser, and transfer agent registered with the Commission to develop, implement, and maintain a comprehensive information security program. The Institute supports this requirement, including its extension to transfer agents. We recommend, however, that the adopting release clarify that a mutual fund complex, which may include the fund's transfer agent, investment adviser, and principal underwriter, each of which is an SEC registrant subject to the revised rule, may develop, implement, and maintain an information security program on a complex-wide basis. As such, each fund or affiliate within the complex that maintains non-public personal information would not be required to have its own unique program so long as it is covered by the program established by the complex. In such instance, the written policies and procedures drafted pursuant to the rule could specify which funds and/or affiliates are governed by the complex's program.

A. Designating the Program Coordinator

The rule would also require each registrant to designate in writing an employee or employees to coordinate the required information security program. The Institute supports this concept but recommends that, rather than requiring the designation of a named individual as coordinator, the rule instead permit a registrant to assign specific responsibility for the program's implementation to either a position that is charged with being the information security program coordinator or to a named

individual. This approach, which is consistent with that adopted by the Commission's sister regulators,[3] will provide registrants the flexibility to assign responsibility to a position within the firm rather than to a specific individual. As such, it will avoid registrants having to revise the written designation whenever one employee succeeds another in coordinating the program, even though the position responsible for such coordination has remained unchanged. The Institute also recommends that the adopting release clarify that, contrary to statements made in the Paperwork Reduction Act portion of the Release, there is no requirement that a board of directors approve the coordinator's designation.[4]

B. Regular Testing

The proposed rule will require each registrant to regularly test or otherwise monitor its program's key controls, systems, and procedures. The Institute strongly recommends that the Commission clarify that, as applied to a registered investment company, the required testing is to be performed as part of the firm's responsibilities under Rule 38a-1 of the Investment Company Act of 1940. This approach will ensure that, as a mutual fund complex implements Regulation S-P's testing requirement, it does so as part of the complex's overall testing of its compliance program. We believe this is an appropriate approach for two reasons. First, the release adopting Rule 38a-1 includes as a required element of a fund's compliance program, "safeguards for the privacy protection of client records and information," which includes the requirements of Regulation S-P.[5] Second, this approach will enable a mutual fund complex to determine, as part of the risk analysis it performs under Rule 38a-1, the level of risk presented to the complex by its information security program and test such program accordingly vis-à-vis its other testing obligations, thereby avoiding an unwarranted concentration of resources for testing done solely pursuant to Rule 248.30.

---

[3] *See, e.g.,* 12 CFR Part 364, Appendix B(III) of the Interagency Guidelines Establishing Standards for Safeguarding Customer Information.

[4] *See* Release at p. 51, where it discusses the Commission's estimate of the hours an institution is expected to devote to compliance. The estimate includes, for smaller firms, "1 hour for the board of directors to designate an information security program coordinator," even though the rule itself includes no such requirement. (For larger firms, 2 hours is allocated to this designation.) The Institute would oppose the rule being revised to require board approval of such person for two reasons. First, it runs contrary to initiatives at the Commission to reduce the ever-increasing duties imposed on mutual fund directors. Second, pursuant to Rule 38a-1 under the Investment Company Act, compliance with Rule 248.30 is a required component of each mutual fund's compliance program. Because a fund's Chief Compliance Officer is approved by the fund's board, it seems unnecessary and inappropriate to have persons who are responsible for discrete functions within the compliance program to also be approved by the fund's board.

[5] *See Compliance Programs of Investment Companies and Investment Advisers,* SEC Release Nos. IA-2204 and IC-26299 (Dec. 17, 2003) at p. 5.

This approach has two other advantages. First, it will enable a mutual fund complex to determine, consistent with its existing compliance program, the appropriateness of relying on a third-party's review of the program (*e.g.,* a SAS 70 conducted of a vendor's program), the need to retain an independent party to conduct a review on the fund's behalf, or the need for the fund to conduct its own tests. Second, it will ensure that information concerning the adequacy of the information security program and any material weaknesses with it are reported to a fund's board of directors.

II. RESPONDING TO UNAUTHORIZED ACCESS OR USE

The Institute strongly supports SEC registrants being required to maintain the confidentiality of consumers' non-public personal information. In our view, however, that the protection of information must be balanced with an appropriate allocation of resources. Indeed, if resources were unlimited, each fund could build a virtual "Fort Knox" around all of its data regardless of the data's sensitivity or vulnerability. Because resources are limited, it is important to ensure the appropriate allocation of resources to protect data and align the protection afforded to data to its sensitivity and vulnerability to theft or misuse. Accordingly, we believe the substantive provisions of the rule should focus on preventing and addressing those security breaches that may adversely impact investors, which are those involving the compromise of sensitive non-public personal information.

We are pleased, therefore, that the rule's definitions recognize a distinction between "personal information" and "*sensitive* personal information" (emphasis added). As defined by the rule, sensitive personal information is 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."[6] Unfortunately, notwithstanding the rule's definitional distinction, its substantive requirements do not go far enough to align the requisite protections with the data's sensitivity and vulnerability. Indeed, most of the provisions in subdivision (a)(4) of the rule, which governs responding to unauthorized access of information, address the compromise of personal information, rather than the compromise of sensitive personal information. There are only two provisions in this subdivision that address the compromise of sensitive personal information. The first is in subdivision (a)(4)(iii), which would require a registrant, after becoming aware of unauthorized access to sensitive personal information, to promptly conduct a reasonable investigation and determine the likelihood that the information has been or will be misused. The second is in subdivision (a)(4)(v), which would require a registrant to notify the Commission on proposed Form SP-30 if "an unauthorized person has intentionally obtained access to or used sensitive personal information."[7]

---

[6] *See* proposed Rule 248.30(d)(10).

[7] Subdivision (a)(4)(iv) requires a registrant that determines that misuse of "the information" has occurred or is reasonably possible to provide notice to individuals pursuant to subdivision (a)(5). While, on its face, this provision appears to apply to all personal information, subdivision (a)(5) only requires that notice be provided in the event sensitive personal information is accessed or used by an unauthorized person. We therefore recommend that subdivision (a)(4)(iv) be revised to replace "the information" with "sensitive personal information."

To ensure that a registrant's compliance dollars are spent where they will have the greatest impact, we recommend that the substantive provisions of the rule be revised to focus on the protection of sensitive personal information. Specifically, the Institute strongly recommends restricting the application of the provisions of proposed Rule 248.30(a)(4) to *sensitive* personal information. This will provide for the diligent protection of information that, if compromised, might result in substantial harm or inconvenience to investors.

We further recommend that subdivision (a)(4) be revised by deleting subpart (a)(4)(B), thereby eliminating any requirement of notice to the Commission merely because an unauthorized person intentionally obtains access to information, even where there is no risk from the access. Consider, for example, a situation in which a wife accesses her husband's account online but there is no substantial harm or inconvenience to the husband as a result of the access. As currently proposed, a registrant may have to provide "notice " of the access to the Commission, even if the registrant determines, after speaking with the husband or other investigation, that the husband has no concerns about the wife's access – perhaps because he provided his account credentials to his wife in the first place. Under our recommended revision, notice to the Commission would only be required if the wife's access resulted in a significant risk of substantial harm or inconvenience to the husband. Revising the notice trigger as we recommend will avoid notices to the Commission in the absence of a significant risk of harm or inconveniences. This seems fitting in light of the Commission's described purpose for notification – *i.e.,* to obtain information about a breach "to determine if an immediate investigation or examination response would be appropriate."[8]

III. NOTIFYING INDIVIDUALS OF UNAUTHORIZED ACCESS AND USE

A. Conditions Triggering Notice to Individuals

Consistent with our comments on subdivision 248.30(a)(4), the Institute is pleased that proposed subdivision 248.30(5) would only require a registrant to notify individuals in the event an individual's "sensitive personal information" has been misused or such misuse is reasonably possible. We recommend, however, that this provision be better tailored to the rule's intent by requiring such notice only in the event that there is a significant risk that the individual identified with the information might suffer, or has suffered, substantial harm or inconvenience.[9] In particular, we recommend that subdivision (a)(5) be amended to delete any requirement of notice to individuals merely because sensitive personal information may have been accessed or used and misuse is

---

[8] Release at p.24.

[9] As discussed below, we additionally recommend that this same standard be utilized to trigger notice to the Commission on proposed Form S-P.

theoretically possible (although there is no real risk of misuse). Instead, notice should only be required in the event there is a significant risk of substantial harm or inconvenience to the individual whose information was accessed.[10]

This amendment is appropriate for two reasons. First, as noted in the Release, the rule is intended to implement the provision in the GLB Act requiring the SEC to impose standards "to protect against unauthorized access to or use of those records or information, which (sic) 'could result in substantial harm or inconvenience to any customer.'"[11] As such, the substantive provisions in the rule should be tailored to instances in which there is a significant risk of such harm occurring, not when there is mere access or use by an unauthorized person. Accordingly, this revision will provide consistency between the GLB Act and the Commission's implementation of it. Second, it will eliminate the proposed nebulous standard of requiring notice whenever misuse of information is "reasonably possible." Indeed, in hindsight, anything could be considered "reasonably possible" and, because of this, registrants may err on the side of sending a notice when the likelihood of misuse of information is remote, but reasonably possible. As recognized in the Release, over-notification of breaches is likely to result in consumers ignoring such notices, perhaps to their detriment.[12] As noted by one commentator, the risk of a notification standard that results in over-notification "would soon teach consumers to ignore [breach notices]. When real danger is threatened, who would listen?"[13] Or, as noted in a 2005 *Washington Post* editorial, "because some of the new [state] laws force disclosure of even trivial breaches, consumers may soon receive so many tedious warnings that they ignore the whole lot."[14]

These concerns are not hypothetical. According to a November 2007 report prepared for the Federal Trade Commission, of individuals surveyed regarding their response to a breach notice received between 2001 and June 2006, 44% "did nothing" about the notice.[15] We suspect, considering the

---

[10] With respect to the "substantial inconvenience" standard in the rule, we recommend that the Commission's adopting release clarify that the appropriate test is not whether any particular individual would consider himself or herself substantially inconvenienced by the breach, but rather, whether a reasonable person would be substantially inconvenienced.

[11] *See* Release at n.9 and related text.

[12] According to the Release, if registrants "are 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." Release at n.49.

[13] *See* Fred H. Cate, *Another notice isn't answer,* USA Today, Feb. 27, 2005 at 14A. *See, also,* Paul M. Schwartz and Edward J. Janger, *Notification of Data Security Breaches,* 105 MICHIGAN LAW REVIEW 913 (Feb. 2, 2007).

[14] *See* Editorial, *Have you been stolen?* WASH. POST (June 30, 2005) at A22.

[15] *See Federal Trade Commission – 2006 Identity Theft Survey Report* (Nov. 2007).

increase in notices since June 2006, the percentage today would likely be higher. Additional factors warranting a more rigorous notification standard include the fact that "only a small percentage of breaches actually involve any harmful use of data" and "information security breaches are among the least common ways that personal information falls into the wrong hands."[16]

B. Timing of the Notices

Pursuant to Rule 248.30(a)(4)(iv), the notice to individuals required by subdivision (a)(5) must occur "as soon as possible," unless delayed at the request of a law enforcement agency. The Institute recommends that the Commission replace the "as soon as possible" standard with a standard requiring notice "without unreasonable delay." This revised standard, which is consistent with state breach notice laws, would better clarify that registrants are not necessarily required to provide notice immediately upon discovering the incident triggering notice. Instead, a notice may be delayed to accommodate a reasonable amount of time for the registrant to conduct an investigation of the incident (to determine its scope and depth), correct any weaknesses or vulnerabilities that may have contributed to the incident, and respond to the incident, including, but not limited to, determining the proper redress to provide to individuals as a result of the incident. Accommodating such a reasonable delay in notifying individuals is appropriate to ensure the completeness of the information communicated at the time of notification and to avoid subsequent communications to the same individuals concerning the same incident. A reasonable delay will also avoid the sending of communications that turn out to be unnecessary in the first place because the investigation and response lead to the conclusion that there was no unauthorized access to sensitive personal information that would require notice.

If the Commission elects not to adopt this recommendation, we strongly recommend that it clarify what is meant by "as soon as possible." For example, does this mean as soon as the registrant is aware of an incident that might trigger notification or as soon as the registrant confirms that the incident does, in fact, trigger notification? Alternatively, does it mean after the registrant has taken each of the steps required by subdivision 248.30(a)(4)? Or, does the Commission intend something else? Regardless of the timing of the notice, we also recommend that the Commission clarify in the adopting release that notice is only required when a fund makes a determination, as required by subdivisions (a)(4)(v) and (a)(5), that there is a significant risk that an individual identified with the information might suffer substantial harm or inconvenience, not when misuse or substantial harm or inconvenience is merely suspected or possible.

C. Responsibility for Providing Notice

As recognized by the service provider provisions in the Commission's proposal, all or part of a registrant's non-public personal information may be maintained by a registrant's service providers. This

---

[16] *See* Fred H. Cate, *Information Security Breaches and the Threat to Consumers,* The Center for Information Policy Leadership, Hunton & Williams LLP (Sept. 2005).

is particularly true of investment company registrants, which have no employees and must rely on service providers to operate. This being the case, when an investment company's shareholder information is maintained by a service provider and accessed by an unauthorized person, there will be an issue as to whether multiple persons (*e.g.,* the fund and the service provider) each have an independent duty to provide notice under Rule 248.30 and, if not, which person has the duty. We recommend that the Commission address and resolve this issue in its adopting release.

In our view, the entity on whose behalf the non-public personal information covered by the rule was collected should be deemed the "owner" of such information and should control who has responsibility for providing notice. We recommend this approach because, in addition to being consistent with state breach laws,[17] we believe the registrant, as the owner of the information, is in the best position to determine the most efficient and least confusing way to notify individuals. For example, if a breach occurs at a service provider with which the affected individuals would have had no direct contact – or even be aware of – a registrant may elect to send the notice because the affected individuals would be familiar with the source of the notice. Notices sent by an entity unknown to the individual would likely confuse the recipient.

Accordingly, we recommend that the Commission address, either in the rule or in the adopting release, two issues relating to providing notice. First, in the event a service provider experiences a breach involving a registrant's non-public personal information, we recommend that the Commission expressly provide that only one entity needs to provide notice of the breach.[18] Second, the Commission should provide that the policies and procedures required of a registrant under Rule 248.30 shall specify either which entity – the owner of the information or the service provider experiencing the breach – shall be responsible for sending the notice or how such decision will be made in the event of a breach.[19]

IV. FORM SP-30

Rule 248.30(a)(4)(v) requires registrants, in the event of more serious breaches, to provide written notice of the incident to the Commission on Form SP-30. The Institute supports the use of a uniform form to notify the Commission of a serious breach. We recommend certain changes, which are described below, to make the reporting more efficient and meaningful.

---

[17] This approach is consistent with that taken under state breach laws. *See, e.g.,* Section 4-110-105 of the Arkansas Code and California Civil Code Section 1798.82.

[18] In the event the fund delegates this responsibility to the service provider, we presume that the fund would have an obligation under Rule 248.30 to ensure the service provider sends such notices in compliance with the rule's requirements.

[19] This may be an issue SEC registrants elect to address in their vendor contracts pursuant to the requirements of subdivision 248.30(a)(3)(vi)(B) or elect to determine on a case-by-case basis depending on what happened in a particular incident.

A. The Form's Contents

As regards the contents of the proposed Form SP-30, we have two overriding concerns. First, it requires more information and detail than necessary to achieve the Commission's purpose of obtaining information about a breach "to determine if an immediate investigation or examination response would be appropriate."[20] For example, the Form requires disclosure of the details concerning the incident, including the personal information compromised and persons involved. It also requires details of account losses, mitigation of customer losses, and net customer losses. This is information that likely will only be available after detailed analysis and resolution of the incident. As such, the Commission's interest is being notified as soon as possible, as the rule requires, is inconsistent with the level of detail the Form requires. This inconsistency can be expected to lead to one of three results: (1) a registrant delaying filing the Form until all the required information is available, thereby thwarting the Commission's interest in prompt notification; (2) prompt filing of the Form, which may result in the Form not being complete due the unavailability at the time of filing of all required information; or (3) multiple filings of the Form on a single incident, with an initial filing being supplemented one or more times as additional information becomes available. Each of these results would result in the Form being a less useful tool to the Commission.

The second concern we have with the Form is the fact that some of its information appears to address specific current issues that may not be issues one, five, or ten years from today. For example, the "pump and dump schemes" referenced in the Form are a relatively recent occurrence in their current form and may not necessarily be a problem in the future. We believe it is inappropriate to include them in a Form that is expected to be in use for many years to come.

To address these concerns, while at the same time preserving the Commission's legitimate interest in being notified of breaches, we recommend that the Commission streamline the Form's contents. We believe that, rather than being a detailed post-mortem notice to the Commission regarding reportable incidents, the Form should instead be used as an early-warning system to notify the Commission of a breach incident experienced by a registrant that involves a significant risk that an individual might suffer substantial harm or inconvenience. The contents of such notice should be limited to a general description of:

- The incident;
- The type of sensitive personal information that may have been subject to unauthorized access or use;
- Acts taken, or being taken, by the registrant in response; and
- Contact information for a person the Commission can contact for additional information.

[20] Release at p.24.

These limited contents will provide the Commission sufficient information to determine, consistent with the stated purpose of the Form, whether an investigation or examination is warranted. Moreover, the general nature of this information reported will enable a registrant to provide notice to the Commission much more quickly than could be accomplished with proposed Form SP-30. Also, once the Commission determines to initiate contact with the registrant in response to a filing, the Commission would have access to the more detailed information it has sought in proposed Form SP-30 as it becomes available during the resolution of the incident. As such, the Commission would have access to any and all information relevant to the incident without requiring it be provided in Form SP-30.

B. Filing Requirements Applicable to the Form

1. Conditions Triggering Notice

As currently proposed, the rule would require that the Commission be notified of a breach in two instances. The first is when there is a significant risk that an individual identified with accessed information might suffer, or has suffered, substantial harm or inconvenience. The second is in the event an unauthorized person has intentionally obtained access to or used sensitive personal information. Consistent with our above recommendation that the rule be revised to require notice to individuals only in the event that there is a significant risk that an individual identified with the information might suffer, or has suffered, substantial harm or inconvenience, we recommend that this same standard be used to trigger notice of a breach to the Commission. As discussed above, using a standard of mere access to or use of information – whether intentional or not – is not consistent with the GLB Act's directive or the rule's intent of protecting investors from substantial harm from data theft or misuse. Moreover, the lower the trigger threshold the more likely notice will be provided to the Commission when notification does not serve the Commission's interest in using notification as a means to "determine if an immediate investigation or examination response would be appropriate." This could make it more difficult for the Commission to discern breaches involving a real threat of identity theft from those that raise no such threat. As a result, the Commission may feel compelled to follow up on each notice it receives, which may result in the unnecessary expenditure of its limited resources with no concomitant public benefit. To avoid this result, we recommend deleting subdivision 248.30(a)(4)(v)(B) and only requiring notice to the Commission in the event there is a significant risk that an unauthorized access to information has resulted or might result in substantial harm or inconvenience to an individual identified with the information.

2. Filing Method

In addition to our concerns with the contents of Form SP-30, we have concerns with the filing requirements applicable to the Form. For example, proposed Rule 248.30(a)(4)(v)(B) and the Release do not disclose how the Form is to be filed – *i.e,* electronically, by fax, in hard copy, or by some other

means. To avoid confusion regarding its filing, we recommend that the rule and/or adopting release provide this detail.

3. Public Access to Filings

Related to the Form's filing is the issue of its access by the public. We have very serious concerns about the information reported on the Form being in the public domain either through the Commission making the information available through its website or EDGAR or in response to a Freedom of Information Act ("FOIA") request. We note that the Release is silent on this issue. In our view, the proposed contents of the Form would require disclosure of very sensitive and confidential information, including information that should *not* be subject to public disclosure. Indeed, a person who has either intentionally accessed sensitive non-public personal information maintained by a registrant or who has an interest in doing so would undoubtedly read such Forms with great interest. There would appear to be no public purpose served by making most, if not all, of the information on Form SP-30 publicly available and we strongly recommend the Commission take whatever steps are necessary to protect the confidentiality of such information. In particular, we recommend that the Commission not publish the Form's contents in any publicly available media and deem such Forms a "nonpublic matter" consistent with Section 17 CFR 200.80(b) of the Commission's rules governing its records and information.[21] If the Commission determines it is appropriate in the public interest to make public certain of the information in the Form, we recommend that it either do so in an aggregated manner without identification of individual information or that the Commission be selective in such disclosure and protect the confidentiality of any sensitive information in the Form that is not appropriate for public disclosure.[22]

C. Immunity for Statements on Form SP-30

The Institute also strongly recommends that the Commission provide an absolute privilege to immunize a registrant from liability in a defamation action for any statements made in a Form SP-30. The immunity we seek is similar to that which is appropriate in connection with a registrant's filing of Form U-5 with FINRA to terminate a representative's registration. We believe this treatment is appropriate to ensure a registrant's complete candor in detailing the information provided on the Form. It is also appropriate because the Form will be filed by registrants participating in a public function.[23]

---

[21] It would appear that, pursuant to 17 CFR 200.80(b)(4) of the Commission's FOIA rules, it would have a sound basis for deeming the contents of Form SP-30 a "nonpublic matter."

[22] One example of this would be the information required by Item 8 of the Form, which requires disclosure of steps a registrant has taken to prevent improper use of any personal information that may have been compromised by the incident. We can see no public interest justifying public disclosure of this information.

[23] This may be an important point for courts considering any defamation suits predicated on information reported on the Form. *See, e.g., Rosenberg v. Metlife,* 866 N.E. 439 (Mar. 29, 2007), involving immunity for statements made on Form U-5.

V. DEFINITIONS

A. Personal Information

The Commission's rulemaking authority for Rule 248.30 – both today and when it was originally adopted in 2000 – can be found in Title V, Section 501 of the GLB Act. This section requires the Commission, and other Federal regulators of financial institutions, "to establish appropriate standards" to:

- Insure the security and confidentiality of *customer* records and information;
- Protect against any anticipated threats or hazards to the security or integrity of such records; and
- Protect against unauthorized access to or use of such records or information which could result in substantial harm or inconvenience to any *customer*. [Emphasis added.]

In other words, the GLB Act governs only the protection of *customer* information. The Commission's current rulemaking under the GLB Act, however, proposes to define "personal information" for purposes of Rule 248.30 in a manner that is inconsistent with the Act. In particular, the Commission has proposed to define this term to include any nonpublic personal information that is identified with *any employee, investor, or securityholder*. The Institute opposes expanding Reg. S-P's provisions to cover persons other than "customers" as such term is used in the authorizing language of the GLB Act.

To begin with, we oppose extending the provisions of Rule 248.30 to cover employees. Because there is nothing in the GLB Act that speaks to the protection of employee information, it appears that, by including such information in Rule 248.30, the Commission has exceeded its rulemaking authority under the GLB Act. We note that, to our knowledge, no other Federal regulator has adopted rules under the GLB Act's safeguarding provisions that address the protection of employee information. To be consistent with its rulemaking authority under the GLB Act, we strongly recommend that the Commission revise its definition of "personal information" to limit its scope to *customer* information.

In addition to concerns with the Commission exceeding its rulemaking authority under the GLB Act, we are concerned with the impact that will result if registrants have to include their employees' information in the registrant's information security program. Because registrants, to date, have not had to include their employees' data in the activities they have undertaken in response to Rule 248.30, to now subject such data to similar requirements will have a significant impact on registrants. This is because the collection, use, and maintenance of such information may occur on systems and through service providers that are different from those utilized for consumers' information. Accordingly, while registrants may have built data security systems around their consumers' information in response to Regulation S-P, they may not have done so to the same degree for their employees' information. To now require them to do so will significantly and unnecessarily increase

their regulatory burdens and compliance costs. To avoid this escalation of cost and ensure that the Commission's rulemaking is consistent with its authority under the GLB Act, we recommend that the definition of "personal information" be revised to conform it to the GLB Act's directives.

We also find the Commission adding "investor" and "securityholder" information to the rule's definition of "personal information" to be most confusing from two perspectives. First, consistent with the GLB Act, since its adoption, Reg. S-P has only addressed "consumers" and "customers" – both of which are defined in the regulation. Importantly, neither term's definition refers to an "investor" or "securityholder." Accordingly, it is not clear why the Commission, in proposing to impose more robust data security standards, has introduced into the regulation two new groups of persons – investors and securityholders. Indeed we are concerned about the confusion that surely will follow regarding what persons these terms are intended to cover that are not currently covered by the regulation's current definitions of consumer and customer.

Second, we are concerned that adding these two new terms may result in inconsistency between the current provisions of Reg. S-P and the proposed revisions to Rule 248.30. For example, currently, Reg. S-P (including the current form of Rule 248.30) does not consider a participant or a beneficiary in an employee benefit plan that is either sponsored by an SEC registrant or for which the registrant acts as trustee or fiduciary to be a consumer or a customer of the registrant. Now that the Commission has proposed to define "personal information" to include information identified with any "investor" or "securityholder," is the Commission intending Rule 248.30 to cover a participant's or beneficiary's information? If so, this would appear to create a confusing and unnecessary internal inconsistency in the regulation's provisions. Moreover, as discussed above, the GLB Act has not authorized the Commission – or other Federal regulators – to address "investor" or "securityholder" information. For the Commission to do so in its current proposal seems to be outside the scope of its lawful authority. Accordingly, in addition to deleting "employees" from the proposed rule, we strongly recommend that the Commission delete any references to investors or securityholders.

B. Sensitive Personal Information

As proposed, the term "sensitive personal information" would mean, in part, personal information that would allow an unauthorized person to use, log into, or access an individual's account, or establish a new account using the individual's identifying information, including the individual's Social Security number. While we appreciate the sensitivity attached to an individual's Social Security number, it is our understanding that, standing alone, the Social Security number is not sufficient to identify and individual, provide unauthorized persons access to an individual's account, or establish a new account. Instead, additional information – including, for example, the individual's name and address – in combination with the Social Security number would be necessary to access or create an account. In recognition of this, we recommend that the Commission revise the definition of "sensitive personal information" in subdivision (d)(10), in relevant part, to read:

> . . . 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 Social Security number, account number, credit or debit card number . . .

This will better ensure protection of the appropriate combination of information that, if compromised, may, in fact, enable an unauthorized person to access an individual's account.

C. Reasonably Possible

We note that the proposed amendments to Rule 248.30 do not include a definition of what is "reasonably possible" with respect to the misuse of compromised information, even though the rule uses this phrase to trigger notice to individuals.[24] While we have recommended that this trigger be eliminated for the reasons stated previously, to the extent it remains in the rule we recommend that the Commission define this term in the rule and that such definition be consistent with the discussion in footnotes 28 and 49 to the Release. Should the Commission elect to delete this term from the rule as we recommend, we recommend that the definition of "substantial harm or inconvenience" be supplemented to add the examples from footnotes 28 and 49 to enable registrants to distinguish unauthorized access that results in substantial harm or inconvenience from unauthorized access that does not result in substantial harm and is not considered to be substantially inconvenient.

VI. TRANSITION/COMPLIANCE PERIOD

The Commission's Release is silent as to an anticipated compliance date or transition period for the revised rule. In our view, it is crucial to the success of the revised version of Rule 248.30 that registrants have sufficient time to implement the totality of its requirements.

According to the Paperwork Reduction Act section of the Release, the Commission's staff estimates that it will take smaller firms 2-80 hours to comply with the totality of the revised rule, with a midpoint of 41 hours.[25] Larger firms are expected to take 40-400 hours, with a midpoint of 220 hours.[26] While we do not have hard data regarding the amount of time needed for compliance, we

---

[24] *See* subdivisions 248.30(a)(4)(iv) and (a)(5).

[25] As previously noted, one hour of this time is allocated "for the board of directors to designate an information security program coordinator," even though the rule includes no such requirement. (Two hours is allocated for this designation in larger firms.)

[26] Interestingly, these estimates include one hour for the program coordinator of a smaller firm to review the amendments and two hours for the program coordinator of a larger firm to review the same amendments.

believe this significantly underestimates both the amount of time and resources needed to comply with the rule. Based on our anecdotal experience, we anticipate that firms will need a compliance period of at least 24 months from adoption of the revised rule. We believe, from talking to our members and by reference to other recent or related rulemaking initiatives of the Commission, that this is a realistic request.

For example, in 2004, when the Commission adopted amendments to Regulation S-P that related solely to the disposal of consumer report information, registrants were provided approximately (1) seven months to implement the amendments and (2) eighteen months to revise their existing contracts with service providers for services involving the disposal or destruction of consumer report information. The 2004 amendments to Regulation S-P did not require an undertaking nearly as extensive or onerous as the Commission's current proposal, which, as discussed below, will require revisions to all contracts with service providers that have access to a registrant's non-public personal information.

Another relevant point of reference is the Commission's 2005 adoption of Rule 22c-2, relating to mutual fund redemption fees. In part, this rule required investment companies to enter into shareholder information agreements with each of their financial intermediaries. In total, the Commission provided investment companies approximately 25 months to have their agreements in place prior to the rule's compliance date. As arduous and burdensome as it was for mutual funds to obtain such agreements with each of their financial intermediaries, such burdens and ardor pale by comparison to what will be entailed by the Commission's proposed revisions to subdivision 248.30(a)(3)(vi). This subdivision will require registrants to have each of their service providers "by contract . . . implement and maintain appropriate safeguards." As defined in the rule, "service provider" includes "*any person* that receives, maintains, processes, or otherwise is permitted to 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." [Emphasis added.] As such, the universe of contracts that will be need to be amended under Rule 248.30 is *far more extensive* than the agreements that had to be executed under Rule 22c-2.

And this is only one aspect of the rule. We strongly recommend that the Commission realistically estimate the time it will take for registrants to develop written policies and procedures to govern their information security programs, evaluate the totality of their "foreseeable internal and external risks," "design and implement safeguards to control [those] risks," "test or otherwise monitor . . . the safeguards' key controls, systems, and procedures" and document compliance with these requirements. Each of these requirements will impose extensive burdens on funds and other registrants and require the allocation of significant resources to complete. Indeed, considering the industry's vast reliance and interdependence on technology – including, for example, desk tops, laptops, websites, PDAs, telephony systems including VOIP and bluetooths, fax machines, and copiers – just conducting

an inventory of all such devices and the security risks they present will be a massive undertaking.[27] In addition, registrants will also have to consider document handling and the "human" element as part of their inventory. Accordingly, the Institute recommends that the adopting release provide registrants ample time – *i.e.,* at least 24 months – to comply with the revised rule's requirements.

VII. INFORMATION SECURITY PROGRAMS OF THE SEC AND THE SROS

The Commission has sought comment on whether it should extend the safeguards and disposal rules to itself and self-regulatory organizations (SROs) or other types of institutions in the securities industry and, if so, which ones. We appreciate the Commission seeking input on this issue and we strongly recommend that the Commission subject itself and each SRO to provisions substantially similar to Rule 248.30.

We note that the Commission and each SRO with inspection authority over SEC registrants may acquire vast amounts of non-public personal information, including sensitive personal information, in connection with each inspection, examination, investigation, regulatory inquiry, or enforcement proceeding. We understand that much of this information may be stored on laptops carried by examiners or on computer systems maintained by the Commission or by one of the many vendors to which the Commission outsources the maintenance of its records. Accordingly, it seems odd to subject information that is held by a registrant to a rigorous information security program while imposing no security requirements by law to such information once it is turned over to the Commission or its staff. We recommend that the Commission address this anomaly.

In making our recommendation, we are cognizant of two recent reports relating to the adequacy of the Commission's current information security practices. One of these reports was published in November 2007 by the Government Accountability Office ("GAO"). It cites the Commission for "significant deficiencies" in its information security controls. According to the GAO's Report,

> . . . [the] SEC has not consistently implemented certain key information security controls to effectively safeguard the confidentiality, integrity, and availability of its financial and sensitive information and information systems. During this year's audit, we identified *continuing and new* information security weaknesses that increase the risk that (1) computer resources (programs and data) will not be adequately protected from unauthorized disclosure, modification, and destruction; (2) access to facilities by unauthorized individuals will not be adequately controlled; and (3) computer resources will not be adequately protected and

[27] According to the Commission's Office of Inspector General, in 2005, the Commission's Office of Information Technology's Asset Management Branch failed to complete an inventory of laptops maintained by Commission personnel "due to resource constraints." *See* n.29, below. The inventory required of registrants under proposed Rule 248.30 will be far more extensive and costly than the laptop inventory the Commission could not afford to complete.

> controlled to ensure the continuity of data processing operations when unexpected interruptions occur. For example, SEC had not yet mitigated weaknesses related to malicious code attacks on SEC workstations, had not yet adequately documented access privileges for a major application, and had not yet implemented an effective intrusion detection system. . . . Collectively, these problems represent a *significant deficiency in the SEC's internal control over information systems and data.* [Emphasis added.][28]

The second report was published in March 2008 by the SEC's Office of Inspector General.[29] According to this report, the Inspector General's "inspection concluded that the [SEC's Office of Information Technology] does not have the proper accountability over laptops" and that "effective accountability of laptop computers simply does not exist." According to the Inspector General, these findings are of concern because "the SEC is privy to an enormous amount of non-public and sensitive market data and most of it is stored on laptops."

While we recommend that the Commission and each SRO be required to adopt a comprehensive and robust information security program, at a minimum, to the extent any person is able to inappropriately access non-public personal information held by the Commission, an SRO, or their staff, the Commission or the SRO should have an express legal duty to notify each registrant whose nonpublic personal information may have been accessed. Such notice will enable the registrant to take whatever action it deems warranted to notify individuals and/or address or mitigate potential misuse of the information. We note that, today, the Commission and the SROs have no duty under state or Federal law to provide such notification. As noted above, however, our recommendation goes beyond mere notification to registrants but extends to the Commission and each SRO having a rigorous information security program substantially similar to that proposed in Rule 248.30.

□ □ □

---

[28] *See Financial Audit, Securities and Exchange Commission's Financial Statements for Fiscal Years 2007 and 2006* (GAO-08-167) (Nov. 2007) at pp.10-11. According to the GAO report, the GAO would be "issuing a separate report on issues [the GAO] identified regarding information security concerns at the SEC." To our knowledge, such a report has not yet been published. By contrast we note that, according to the report of *The President's Identity Theft Task Force, Combating Identity Theft* (April 2007) , "The SEC has not yet found any deficiencies during its examinations of [SEC registrants] that warranted formal enforce actions [under Regulation S-P] . . .." *See* Volume II of the report at p.13.

[29] *See Control Over Laptops,* SEC Office of Inspector General (Inspection Report No. 441, March 31, 2008). The Inspector General's report includes five recommendations for the Commission to implement to enhance the security associated with Commission laptops. We commend the Commission's staff for its expressed interest in implementing these recommendations but hope that the Commission will also adopt an information security program substantively similar to that proposed for registrants.

The Institute appreciates the opportunity to comment on this proposal. If you have any questions concerning our comments, please contact me at 202-326-5825 or Bob Grohowski of the Institute at 202-371-5430.

Sincerely,

/s/ Tamara K. Salmon

Tamara K. Salmon
Senior Associate Counsel

cc: Erik R. Sirri, Director
Division of Trading and Markets

Andrew J. Donohue, Director
Penelope Saltzman, Acting Assistant Director, Office of Regulatory Policy
Vincent Meehan, Senior Counsel, Office of Regulatory Policy
Division of Investment Management