T. ROWE PRICE ASSOCIATES, INC.

LEGAL DEPARTMENT

WWW.TROWEPRICE.COM

P.O. Box 89000
Baltimore, Maryland
21289-1020

100 East Pratt Street
Baltimore, Maryland
21202-1009

Toll Free 800-638-7890
Fax 410-345-6575

May 12, 2008

Via Electronic Mail

Ms. Nancy M. Morris
Secretary
U.S. Securities & Exchange Commission
100 F Street, N.E.
Washington, DC 20549

Re: Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Personal Information (File No. S7-06-08)

Dear Ms. Morris:

T. Rowe Price[1] appreciates the opportunity to submit comments and offer our views on the above-referenced proposed amendments to Regulation S-P ("**Proposal**").[2] As of March 31, 2008, T. Rowe Price's assets under management were approximately $378 billion, with assets of approximately $230 billion invested in the T. Rowe Price family of mutual funds (comprised of over 120 funds with over 10.9 million shareholder accounts).

The Proposal primarily involves the replacement of the existing data security provisions in Regulation S-P ("**Reg. S-P**"), 17 C.F.R. § 248.30,[3] with more detailed and expanded provisions. The provisions, both current and proposed, have two main components that are derived from two different laws: the so-called "Safeguards Rule" under Title V, Subtitle A of the Gramm-Leach-

[1] For purposes of this letter, "T. Rowe Price" refers to the following entities: T. Rowe Price funds, consisting of over 120 registered investment companies; T. Rowe Price Associates, Inc., which serves as investment adviser for the T. Rowe Price funds (other than the international funds) as well as provides investment management services to other clients; T. Rowe Price Investment Services, Inc., which serves as principal underwriter and distributor for the T. Rowe Price funds and provides brokerage services to the funds' shareholders and other retail customers as an introducing broker through its Brokerage Division and offers two proprietary no-load variable annuity products and Section 529 College Savings Plans for two different states; T. Rowe Price Services, Inc., which acts as the registered transfer agent for the T. Rowe Price funds and provides shareholder and administrative services for the funds; and T. Rowe Price Retirement Plan Services, Inc., which is also a registered transfer agent and provides recordkeeping and administrative services for employer-sponsored retirement plans investing in the T. Rowe Price funds and other outside funds.

[2] 73 Fed. Reg. 13,692 (Mar. 13, 2008).

[3] Throughout this letter, further references to 17 C.F.R. pt. 248 will be noted simply by section number (e.g., § 248.30).

Bliley Act ("**GLBA**"),[4] and the "Disposal Rule" under the Fair and Accurate Credit Transactions Act of 2003 ("**FACT Act**").[5] Generally, the Safeguards Rule requires the establishment of policies and procedures to address administrative, technical, and physical safeguards for the protection of customer records and information under Reg. S-P, while the Disposal Rule focuses on disposal of consumer reports and information derived from consumer reports by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. References in this letter to the "**Rules**" mean the Safeguards and Disposal Rules collectively.

We appreciate the efforts the Commission has made in making the Proposal consistent with many aspects of the equivalent safeguards and disposal rules adopted in past years by the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of Thrift Supervision (collectively, the "**Banking Agencies**"), and the Federal Trade Commission ("**FTC**"). We support Commission's intention to replace the existing provisions of § 248.30 with more robust Rules. However, we recommend that the Commission:

- Clarify that each covered institution in a complex or family of companies may develop or rely on a common information security program if they so choose, and need not separately document and test, for example, common elements of the program;
- Limit coverage of the Rules to information related to customers, and not expand the Rules to information related to consumers, employees, investors, or securityholders;
- Remove direct coverage of transfer agents from the Proposal, or as an alternative, exclude transfer agents when acting for one or more investment companies already subject to the Rules;
- Remove direct and separate application of the Disposal Rule to associated persons of a broker or dealer, supervised persons or a registered investment adviser, and associated persons of a registered transfer agent;
- Adopt certain changes recommended by the Investment Company Institute in its letter to the Commission dated May 2, 2008;
- Clarify that affiliated companies need provide only one notice to the Commission and one notice to the impacted individual when the one or more of the companies is involved in a privacy incident;
- Clarify the Rules' testing requirements;
- Allow institutions to designate a "person or persons" to coordinate programs, which may be indicated by name, position, or office;

[4] 15 U.S.C. 6801 *et seq.*

[5] 15 U.S.C. 1681w.

- Remove requirements to maintain specific written records, or as an alternative, include separate recordkeeping requirements for the Rules, which would be consistent for all entities subject to the Rules and which would be deemed to apply instead of such entities' other general recordkeeping requirements;
- Adopt specified changes to certain definitions; and
- Provide a sufficient period before final Rules would become effective.

Each of these recommendations is discussed in detail below.

I. Avoid Duplication of Efforts and Unnecessary Burdens Regarding "Service Providers"

The T. Rowe Price family of mutual funds and up to four other T. Rowe Price corporate entities would be subject to these provisions. There are outside service providers that some or all of them use jointly (e.g., an off-site document storage vendor) and many procedures for safeguarding that are implemented on a complex-wide basis as opposed to a legal entity basis (e.g., building security, training, method of securing employee and customer usernames and passwords, Internet firewalls and virus detection). We are extremely concerned by the Commission's statement that affiliates providing services complex-wide would be deemed to be "service providers" to each covered institution and that "each" institution subject to Reg. S-P would be responsible for taking reasonable steps to ensure the service provider is capable of maintaining appropriate safeguards and to oversee the service provider.[6]

We strongly urge the Commission to make clear in the regulation that each covered institution in a complex or family of companies may develop or rely on a common information security program if they so choose, and need not separately document and test, for example, common elements of the program. We see increased costs and unnecessary burdens, but no benefits, in requiring "each" institution in a complex to take (and presumably document) reasonable steps in the selection and oversight of service providers. Institutions that are part of a complex are in a unique position to gauge, on a daily basis, the effectiveness of activities provided by a centralized department that may, in fact, be under the technical corporate umbrella of an affiliate, and they can gauge the effectiveness in a way that is simply not possible vis-à-vis unaffiliated third-party service providers.

For example, the facilities management department for the T. Rowe Price family of companies maintains, evaluates, and updates written procedures regarding appropriate building security protocols for all locations. It makes no sense for each mutual fund, the broker-dealer, the investment adviser, and the transfer agents to duplicate these procedures and for each one to separately evaluate that department. As a large financial services provider, we rely on the expertise of many departments, which may be under different legal entities, to evaluate and design processes and procedures that we then apply complex-wide when appropriate. Similarly,

[6] 73 Fed. Reg. at 13,696.

the T. Rowe Price funds and all other covered financial institutions in the complex use the same outside service provider for off-site storage of documents. We do not believe that any purpose would be served in requiring more than 125 affiliated institutions to evaluate and monitor this provider as long as the evaluation and monitoring is done on behalf of the complex itself.

II. Proposal to Expand the Scope of Information Covered by, and Entities Subject to, Various Aspects of the Rules

(A) Proposal to Expand the Scope of Information Covered by the Rules: The Proposal would require safeguarding and appropriate disposal of "personal information," a new term that would encompass any record containing either "nonpublic personal information" ("**NPI**") or "consumer report information" as those terms are defined currently in Reg. S-P. This change would expand the express scope of the Disposal Rule to encompass NPI, and not simply consumer report information, but we agree with the Commission that a properly structured information security program under the Safeguards Rule would need to address prudent practices when disposing of NPI in any event.[7]

However, an expansion into four new types of information to be covered by the Rules is contemplated through an amendment to an existing term, "personally identifiable financial information" ("**PIFI**"), which, in turn, is a subset of NPI. More specifically, the definition of PIFI would be amended to add any information "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."[8] The Commission asked respondents whether they believed such an expansion should be made or whether the scope should be limited to information relating to customers of an institution.

We believe that coverage should be limited to information relating to customers of an institution. This coverage, and not expanded coverage, is authorized by the GLBA. The current Safeguards Rule applies to customers, as do the long-standing equivalent rules of the Banking Agencies and the FTC. Subtitle A of the GLBA expressly directs the establishment of regulations to "insure the security and confidentiality of customer records and information."[9] Subtitle B similarly directs the Commission and other agencies to prescribe regulations and guidance "to prevent the

---

[7] While use of the new term "personal information" also would appear to expand the scope of the Safeguards Rule to include consumer report information and not just NPI, we note that "information from a consumer report" is already within the scope of NPI under Reg. S-P. § 248.3(t)(1)(i), .3(u)(2)(i)(G).

[8] Proposed § 248.3(u)(1)(iv).

[9] 15 U.S.C. 6801(b)(1).

unauthorized disclosure of customer financial information," as well as to deter and detect identity theft activities relating to "customer information of a financial institution."[10]

In addition to concerns over whether the SEC has the authority to expand coverage to these four new groups, we note further concerns below.[11]

(1) Coverage of information "identified with any consumer": The phrase "that is identified with any consumer" is unnecessary and potentially inconsistent and/or confusing in light of the fact that the definitions of "consumer report information" and NPI already define the scope of each and no changes are proposed to either of these definitions. "Consumer report information" covers specified information "about an individual."[12] The definition of NPI uses the term "consumer" throughout, as does PIFI, which is a subset of NPI.[13] "Consumer" is already a defined term in Reg. S-P with many useful examples.[14] Unlike the Banking Agencies and the FTC, which limited the scope of their safeguards rules to NPI concerning customers, the Commission, by not including this limitation, already has proposed to cover consumers and consumer relationships as long defined by Reg. S-P. In adding another reference to consumers to the definition of PIFI, does the Commission intend some other type of information or is there an intention to alter the scope of existing definitions or examples in some way? There does not appear to be such an intention stated by the Commission in the Supplementary Information published with the Proposal. Accordingly, we recommend that the phrase not be added.

(2) Coverage of information "identified with any employee": In proposing to expand the scope of information covered by the Rules to employee information, the Commission noted that the definition would include records of usernames and passwords and other information that would allow a thief to impersonate an employee or employ "social engineering" techniques or bribery.[15] While we understand the Commission's goals, we believe that adding to the scope any information identified with any employee is overly broad. We believe, for

---

[10] 15 U.S.C. 6825; 6821(a). The definitions used in Subtitle B make clear that the Subtitle covers direct customers of financial institutions. *See, e.g.,* 15 U.S.C. 6828 (definitions of "customer," "customer information of a financial institution," and "financial institution").

[11] In addition to not adopting proposed § 248.3(u)(1)(iv) (i.e., addition of these terms to the definition of PIFI), conforming changes would be needed to proposed § 248.30(a)(2)(iii) and .30(d)(8) which include references to these four groups as well.

[12] § 248.30(b)(1)(i). This is consistent with the language of the FACT Act, 15 U.S.C. 1681w. In the Proposal, the current definition is used without change, but is relocated to proposed § 248.30(d)(4).

[13] § 248.3(t), .3(u). This is consistent with the scope of Subtitle A of GLBA pursuant to which the existing Safeguards Rule was enacted.

[14] § 248.3(g).

[15] 73 Fed. Reg. at 13,700.

example, that any adequate information security program already would have to address appropriate security for usernames and passwords, whether they are the usernames and passwords of the customers themselves or of employees providing service to customers. Neither the Banking Agencies nor the FTC has included employee information as a separate category in their equivalent rules.

We believe that companies have an interest in protecting employee information for many reasons and that they do so on a regular basis. However, areas and systems with other employee information (e.g., payroll) frequently are different than those that house customer information. This change would greatly expand the scope of the Rules and the attendant burdens on those subject to Reg. S-P in a way that does not justify the costs. For example, T. Rowe Price has a computerized system whereby employees can be nominated and recognized for significant achievements. Under the very broad language used in the Proposal, would this system be covered? We believe the inclusion of employee information as a separate category should be removed.

(3) Coverage of information "identified with any investor or securityholder who is a natural person": The definition PIFI would be expanded to include any information that is identified with any "investor or securityholder who is a natural person." There are several troubling aspects to this part of the proposed expansion. First, while it appears the terms are being added in relation to transfer agents, there is no such limitation stated in the proposed regulation itself and as a result, they would apply to broker-dealers, investment advisers, and investment companies as well. Second, there are no definitions of these terms and no direction as to the type of investor or securityholder intended to be covered. For example, would this potentially include natural persons who are holders of the corporate stock of a broker-dealer, investment adviser, or transfer agent, persons completely beyond the scope of the GLBA? For investment companies, how would this expansion interact, for example, with existing provision in § 248.3(g)(2)(iv), which provides that an individual is not a consumer of an investment company when the individual purchases shares through a broker-dealer or investment adviser who is the record owner?

Third, even expressly limiting coverage of these terms to transfer agents is problematic. The term "investor" is not used in connection with the laws or rules governing transfer agents and should be removed. The term "securityholder" is used in the laws and rules governing transfer agents, but its inclusion into the existing definition of PIFI is confusing. PIFI is part of an interlocking set of definitions in Reg. S-P—primarily "consumer," "customer," and NPI. Each has useful examples of what is deemed to fall within, and outside of, their respective spheres. By adding to the scope of § 248.30 any information identified with a "securityholder who is a natural person," what would happen to existing Reg. S-P treatment of persons deemed inside and outside the scope of Reg. S-P and the Safeguards Rule?

For example, currently Reg. S-P (including its Safeguards Rule) does not consider a participant or a beneficiary in an employee benefit plan that is either sponsored by an institution or for which the institution acts as trustee or fiduciary to be a consumer or customer of the institution.[16] As noted by the SEC in its adopting release to Reg. S-P in June 2000, among the reasons for the exclusion was that the customer of the financial institution is the plan or trust itself and by acting as trustee, the financial institution already has taken on obligations of a fiduciary, including the duty to protect confidential information.[17] Does the Commission now intend for the first time to cover a participant's or beneficiary's information to the extent held by a transfer agent, even though the securityholder remains the plan itself?[18] Such a change would be completely contrary to the safeguard rules adopted by the Banking Agencies and the FTC. Accordingly, we recommend that the Commission remove coverage of "securityholder" information as well, or, as an alternative, carefully evaluate and specify how the term interacts with all aspects of the definitions and examples used for "consumer," "customer," NPI, and PIFI.[19]

(B) Proposal to Expand the Scope of Institutions Covered by the Safeguards Rule: The Commission proposes to extend the Safeguards Rule to transfer agents. They already are subject to the Disposal Rule consistent with the FACT Act. The Commission states that it is doing so under its general rulemaking authority conferred by Section 17A of the Securities Exchange Act of 1934.[20] As noted in Part II(A)(3) above, we have recommended that the scope of information covered by the Rules not include information relating to "investors" and "securityholders." If these are removed, there does not appear to be any reason to expand the scope of the Safeguards Rule to apply directly to transfer agents.

If the Commission decides to retain the expansion to transfer agents, we urge the Commission to exclude transfer agents when they are acting for one or more investment companies already subject to the Safeguards Rule. This would avoid potential confusion and overlapping duties

---

[16] § 248.3(g)(2)(viii).

[17] 65 Fed. Reg. 40,334, 40,339 (Jun. 29, 2000).

[18] And, similar to other examples noted earlier in this subpart of the letter, does it somehow change the long-standing rules for other institutions subject to the Safeguards Rule?

[19] These same concerns exist as to the term "investor." To the extent the term is not removed, we would ask the Commission to carefully evaluate and specify how that term interacts with the other definitions and examples noted.

[20] The Commission expressly does not have such authority under Subtitle A of the GLBA as it was only granted authority as to broker-dealers, investment companies, and investment advisers. 15 U.S.C. 6804(a), 6805(a)(3 - 5). While the SEC also has rulemaking authority under Subtitle B of the GLBA, expansion to directly cover transfer agents would not appear to be consistent with Subsection B's focus on financial institutions with direct customer relationships as discussed in note 10 above.

without lessening protections to those currently covered by the Safeguards Rule.[21] For example, in the case of a transfer agent that is acting in connection with the shares of an investment company, direct coverage of both entities would lead to duplication of information security programs and notices. There also is no apparent purpose in subjecting this one category of an investment company's service providers to direct coverage under the Safeguards Rule as opposed to other categories of service providers (for example, the provider of a recordkeeping system that has access to extensive customer data).

Investment companies already have duties regarding the use and oversight of service providers, and these would be further detailed under the Proposal. Indeed, for investment companies, which have no employees, it makes sense for the company or mutual fund complex to develop, implement, and maintain an information security program on a complex-wide basis in close conjunction with its transfer agent. Regardless of what the Commission decides on this issue, we recommend that this approach be identified as an acceptable method of compliance in the final regulation or adopting release.[22] However, we reiterate that removing transfer agents when acting for investment companies from the scope of direct coverage of the Safeguards Rule as proposed would not reduce protections applicable to consumers and customers of investment companies—the investment companies would remain ultimately responsible for safeguarding information and ensuring compliance by all of their service providers, including their transfer agents.

(C) Proposal to Expand the Scope of Persons Covered by the Disposal Rule: The Commission proposes to expand persons subject to the Disposal Rule to natural persons who are associated persons of a broker or dealer, supervised persons or a registered investment adviser, and associated persons of a registered transfer agent. The Commission noted its concerns that some persons, who may work in remote branches, may not dispose of information consistent with the institution's disposal policy. We are opposed to singling out such persons and believe it sends the wrong message to institutions and their employees regarding the Rules.

In developing information security programs, including disposal methods, institutions should take into account the needs and differences of remote branches and offices and not offer a "one size" solution unless the one size actually "fits all." This may mean that a main office with significant operations uses a comprehensive shredding/pulping program while a remote office with insignificant disposal volumes may use a good quality, cross-cut shredder purchased at a local office supply store. The institution, in developing a program appropriate to its size and complexity, should evaluate all locations and develop corresponding protocols not only for disposal, but also for safeguarding.

---

[21] Additionally, if the coverage of "investor" and "securityholder" information is not removed for the reasons noted in Part II(A)(3), this approach would serve to avoid potentially conflicting standards between investment companies and the transfer agents that act for them.

[22] See also Part I above on this issue.

We stress to all of our employees that they must comply with all aspects of our information security protocols that are applicable to them and their respective locations. For example, they must comply with the duty to keep usernames and passwords confidential, rather than only complying with disposal aspects of our program. The Banking Agencies and FTC have not singled out employees for the disposal (or safeguards) aspects of their rules. Also, as regards associated persons of a transfer agent, the definition in Section 3(a)(49) of the Securities Exchange Act of 1934 excludes employees whose functions are solely clerical or ministerial. Similarly, such employees are largely excluded from being deemed to be associated persons of a broker or dealer under Section 3(a)(18) of the Securities Exchange Act of 1934. We do not believe the Commission intends to exclude such persons to the extent that they come into contact with confidential information. For these reasons, we do not believe it is necessary or beneficial to single out natural persons who are associated persons of a broker or dealer, supervised persons or a registered investment adviser, and associated persons of a registered transfer agent for direct compliance with the Disposal Rule.

III. Components of the Information Security Program

We support many aspects of proposed Section 248.30(a) regarding the components of an information security program. The main elements are the development, implementation, and maintenance of a comprehensive information security program for the safeguarding of personal information and for responding to unauthorized access to or use of personal information.

Regarding proposed Section 248.30(a), we agree with the comments and concerns raised by the Investment Company Institute ("**ICI**") in its letter to the Commission dated May 2, 2008 concerning:

- Consistently aligning the provisions of proposed § 248.30(a)(4) regarding incident response to "sensitive personal information" as opposed to "personal information" as is sometimes used.
- Removing proposed § 248.30(a)(4)(v)(B) so that the Commission need not be notified of an incident involving intentional access to or use of sensitive information when, due to the particular facts of the case, there is not a significant risk of substantial harm or inconvenience.[23]
- As to the timing of notices to individuals, replace the "as soon as possible" standard in proposed § 248.30(a)(4)(iv) with a standard of "without unreasonable delay." For example, sufficient time is needed to conduct discovery of the incident and take steps to protect information from further unauthorized access or use—information required to be contained in the notice to the individual.

[23] Stated another way, reporting to the Commission should be required only when notification to the impacted individual is required.

- Greatly simplifying proposed Form SP-30 and specifying acceptable filing methods.[24]
- Restricting public access to filed Form SP-30s and providing an absolute privilege from potential defamation liability.

We have additional suggestions and concerns as noted below.

(A) Obligation to Provide Notice: Similar to the points raised above in Part I, we believe that it is appropriate and cost-effective when affiliated companies are involved in a privacy incident to provide one Form SP-30 to the Commission and one notice to an individual if they so choose. We also believe that institutions should be permitted to delegate the notice requirements to each other or to an appropriate service provider. For example, if there is an incident with an individual that compromises his or her sensitive personal information involving three separate mutual funds and an advisory service all within the T. Rowe Price complex, it would serve no purpose for up to five notices to be made to the Commission and the individual (one from each investment company, one from the adviser, and as currently drafted, one from the transfer agent of the mutual funds). Indeed, the individual may be left with the impression that there were five separate incidents. Only one notice to the Commission and one notice to the individual should be required as long as the notice makes clear the accounts or services at issue.[25]

(B) Provisions Regarding Testing and Monitoring: Proposed § 248.30(a)(3)(iv) requires institutions to "regularly test or otherwise monitor" the effectiveness of the system. The term "regularly" also is used in the safeguards rule of the Banking Agencies and the FTC. While none of these agencies have defined the term (nor does the Commission propose to do so), the Banking Agencies' regulations have a reference to frequency and nature being determined in connection an institution's risk assessment.[26] Depending on the activity at issue, an institution's risk assessment may indicate that an annual review is warranted, or a period that is more or less frequent. We recommend that the Commission add similar language to proposed § 248.30(a)(3)(iv).

Also, as noted in Part I above, we urge to Commission specify that institutions that are part of a complex using common program elements need not separately test and monitor. Similarly, a chief compliance officer should be able to rely on a complex-wide assessment for purposes of: (i) Rule 38a-1 of the Investment Company Act of 1940 for investment companies; (ii) FINRA's NASD Rule 3013(b) for broker-dealers; and (iii) Rule 206(4)-7 of the Investment Advisers Act

[24] An alternative would be to adopt the approach of the Banking Agencies where a phone call will suffice. The Agencies noted that they wanted maximum flexibility and did not want to create "another SAR-like process that requires the completion of detailed forms." 70 Fed. Reg. 15,736, 15,741 (Mar. 29, 2005).

[25] In addition to the changes to Form SP-30 recommended by the ICI, the Commission should allow for identification of multiple institutions or a fund complex that are jointly reporting the same incident.

[26] See, e.g., 12 C.F.R. pt. 570, App. B, subpt. III.C.3 (safeguards rule of the Office of Thrift Supervision, providing that "[t]he frequency and nature of such tests should be determined by your risk assessment").

of 1940 for investment advisers. We believe this approach appropriately will allow institutions to test and/or monitor in conjunction with their other testing and monitoring obligations, thereby avoiding an unwarranted concentration of resources for testing done solely for these Rules.

(C) Designation of "Employee or Employees" to Coordinate the Program: The Commission asked whether the requirement in § 248.30(a)(3)(i) to designate an employee or employees to coordinate the program should specify that this may be done by name, position, or office. We agree with this approach, but in light of the fact that investment companies do not have employees, we recommend that the broader term "person" be used instead."[27] This also would provide flexibility to a large complex with multiple types of institutions to have a single "Chief Privacy Officer" if they so choose. Accordingly, we recommend that the language in this subsection be revised to read: "Designate in writing ~~an employee or employees~~ a person or persons, which may be indicated by name, position, or office, to coordinate your information security program".

IV. Maintenance of Written Records

Eight subsections of proposed Section 248.30 have individual requirements to "maintain written records" and then there are detailed rules as to how records are to be maintained.[28] There are no such requirements in the equivalent rules of the Banking Agencies and the FTC. We believe the institutions subject to Reg. S-P are cognizant of the need to document and retain appropriate records to generally illustrate how their policies and procedures are designed to ensure compliance with regulations, regardless of whether the regulation at issue specifies any particular recordkeeping.[29] The magnitude and specificity of written records under the Proposal threatens to divert resources and time to the creation and maintenance of these specific records instead of the design and maintenance of robust safeguarding and incident response systems.

---

[27] This is consistent with the language used in the Anti-Money Laundering Program requirements for investment companies, 31 C.F.R. § 103.130(c)(3) ("designate a person or persons responsible").

[28] Proposed § 248.30(a)(3)(iii) (design and implement safeguards to control identified risks and "maintain a written record of your design"); 248.30(a)(3)(iv) ("maintain a written record of the effectiveness of the safeguards' key controls, systems, and procedures"); 248.30(a)(3)(vi) (oversee your service providers and "document in writing in your oversight" that you are meeting specified steps); 248.30(a)(4)(i) ("maintain a written record of the personal information systems and types of personal information that may have been accessed or misused"); 248.30(a)(4)(ii) ("maintain a written record of the steps you take" to contain and control an incident of unauthorized access or use of personal information); 248.30(a)(4)(iii) ("maintain a written record of your determination" regarding the likelihood that personal information has been or will be misused); 248.30(a)(4)(iv) ("maintain a written record that you provided notification" to individuals regarding the misuse or possible misuse of their personal information); and 248.30(b)(2)(ii) ("document in writing its proper disposal" of personal information). Proposed § 248.30(c) then specifies that records are to be maintained in the manner required under other, existing recordkeeping rules for the type of institution at issue.

[29] For example, none of the other sections of Reg. S-P, which have been in place since 2000, have specific recordkeeping requirements.

As examples, the language in proposed Section 248.30(a)(4)(ii) to "maintain a written record of the steps you take" to contain and control an incident involving unauthorized access or use may be interpreted to require the creation and maintenance of a detailed record of the exact steps of recoding a personal information system that mismatched two customer records. What is important is that the source is discovered, corrected, and tested. To divert precious time and resources to capturing pages of computer coding, for example, does not serve the overall purpose of the Rules. When there is a requirement in proposed Section 248.30(a)(4)(iv) to "maintain a written record that you have provided notification" to an impacted individual, does this require time-consuming and expensive certified mail, return receipt requested? Does it require that you maintain a log of letters instead of just copies of the letters themselves? To comply with proposed Section 248.30(b)(2)(ii) regarding the need to "document in writing its proper disposal of personal information," is there a need to maintain a log of every piece of paper placed into a secure shred/recycle bin? The fact that such a system is in place, is required to be used through written procedures, and is generally monitored should be sufficient instead of this provision.

We urge the Commission to remove the references to maintaining records in all of these subsections and allow institutions flexibility in documenting their efforts to comply with the Rules. This also would make the requirements consistent with the Banking Agencies and FTC and further the provisions in the GLBA and FACT Act for coordination of regulations when possible across all of the regulators.[30] Should the Commission find in the future that this approach is not sufficient, it can provide guidance or amend Reg. S-P in a more targeted manner.

To the extent these references are not removed, we are concerned about the requirement in proposed § 248.30(c) that each entity subject to the Rules preserve the records in accordance with each entity's generally-applicable recordkeeping rules. The recordkeeping rules for each of these entities vary with respect to the length of time and manner in which the records must be maintained, especially with respect to records preserved in electronic format, the method likely used for records preserved under Reg. S-P. Maintaining these records in compliance with each of these recordkeeping rules would be burdensome for mutual fund complexes with different types of entities subject to the Rules. For example, for a complex like T. Rowe Price, with registered investment companies and mutual fund transfer agents, a registered investment adviser, and a broker-dealer, the records required under the Rules would need to be maintained in accordance with four different recordkeeping rules, each with varying requirements.[31]

Each of these T. Rowe Price entities uses assorted recordkeeping systems to preserve their records in accordance with applicable recordkeeping rules. In some cases the systems are separate and in other cases two or more entities may use the same recordkeeping system for certain types of records. In addition, the broker-dealer's and transfer agents' systems use two

[30] 15 U.S.C. 6804(a)(2) (GLBA); 15 U.S.C. 1681w(a)(2) (FACT Act).

[31] 17 C.F.R §§ 240.17a-4(b); 240.17Ad-7(b); 270.31a-2(a)(4); 275.204-2(c)(1).

different third parties to fulfill the third party access requirement mandated under each of their applicable electronic recordkeeping rules.[32] It would be extremely burdensome and redundant for a mutual fund complex to maintain the records required under § 248.30 in various systems under varying requirements for varied periods of time. In addition, because the transfer agent recordkeeping rules generally apply to records for securityholder accounts, the systems designed to preserve these records are "account-based," not "incident or policy based" (i.e., records are scanned and indexed to a particular shareholder account). As such, the records required under the Proposal are not conducive to being preserved in the manner that mutual fund transfer agents typically follow to maintain their electronic records. It is likely that significant system changes would need to be made to accommodate maintaining the records required under § 248.30 in compliance with the transfer agents' recordkeeping rules.

For the reasons stated above, we recommend the proposed Rules be revised to remove all specific recordkeeping requirements and references or, as an alternative, that the Rules have their own recordkeeping requirements, which would be consistent for all entities subject to the Rules and which would be deemed to apply instead of such entities' other general recordkeeping requirements.

V. Other Technical Changes to Definitions

(A) "Sensitive Personal Information": We agree with the ICI that a Social Security number standing alone would not allow access to an account or aid identity theft. It is simply a string of nine digits. We support the revisions the ICI has recommended to proposed Section 248.30(d)(10).

(B) "Substantial Harm or Inconvenience": We recommend three changes to proposed Section 248.30(d)(12) regarding the definition of "substantial harm or inconvenience." First, we recommend that the last phrase of subsection (ii) be changed to read: "such as if the use results ~~only~~ in ~~your deciding~~ a decision by you or the individual to change the individual's account number or password." For example, an institution notifying a customer of an event that does not raise significant concerns may leave it up to the customer to decide whether or not to change an account number. Second, we recommend that the examples provided in footnotes 28 and 49 of the Proposal be added as additional examples in subsection (ii). Last, there should be language added to make clear that "substantial harm or inconvenience" is evaluated based on whether a reasonable person would be substantially harmed or inconvenienced.

VI. Implementation Period

We recognize that under the current Rules, covered institutions should have many aspects of the Rules as proposed already in place. However, some aspects are completely new, such as the implementation of an incident response program and coverage of NPI by the Disposal Rule.

[32] 17 C.F.R §§ 240.17a-4(f)(3)(vii); 240.17Ad-7(f)(5).

Even for concepts that are not new, the sheer additional detail added will take time to analyze against existing program components and possibly lead to further work. To the extent that the Commission does not remove direct coverage of transfer agents, the Safeguards Rule will be new for them. Similarly, if coverage of employee, investor and securityholder data is not removed, this would be new to all covered institutions.

When the FTC adopted its safeguards rule in 2002, it provided for a one-year delayed effective date.[33] We recommend that there be at least a 12-18 month delayed effective date for any final regulation. As an example, a few years ago T. Rowe Price designed and implemented a complex-wide privacy incident reporting system to allow for centralized reporting, resolution, escalation, and notification to customers where warranted. The design, implementation, testing, and training process took approximately nine months, and we were able to move that quickly only through the consistent efforts of an interdisciplinary team. Even though we have an incident response system, it will take time to review our system against final Rules and make changes as needed. For example, the system was designed without the need to comply with layers of competing recordkeeping rules. While we are a large organization, we believe the development of a new program will take time even for a small organization, especially in light of what are likely to be limited personnel and resources. For these reasons, a sufficient implementation period is needed.

We appreciate the opportunity to comment on the Commission's proposed amendments to Reg. S-P. If you have any questions concerning our comment letter, or need additional information, please feel free to contact either of the undersigned. We would welcome an opportunity to meet with staff members at the Commission to share information on some of the unique challenges a large organization would face under the Proposal.

Sincerely,

David Oestreicher
Chief Legal Counsel
410-345-2628

Karen Nash-Goetz
Associate Legal Counsel
410-345-2260

[33] 67 Fed. Reg. 36,484 (May 23, 2002). We note that the FTC's rule is simplified and does not have an incident response and notification component.