National Association for Information Destruction, Inc.
3420 East Shea Blvd., Suite 115, Phoenix, Arizona 85028
Phone: (602) 788-6243 Facsimile: (602) 788-4144
Email: exedir@naidonline.org Website: www.naidonline.org

April 18, 2008

BY ELECTRONIC FILING

Securities and Exchange Commission
Nancy M. Morris, Secretary
100 F Street, N.E.
Washington, DC 20549-1090

Re: Comments on Proposed Amendments to Regulation S-P
File Number S7-06-08

To the Commission:

The National Association for Information Destruction, Inc. ("NAID") submits these comments on the Securities and Exchange Commission's ("SEC" or "Commission") proposed rule to amend Regulation S-P: Privacy of Customer Financial Information and Safeguarding Personal Information.[1] The National Association for Information Destruction, Inc. ("NAID") is the international, non-profit trade association of the information destruction industry. NAID's members include individuals as well as large and small businesses that provide information destruction services. NAID and its members are expert in, and committed to, the proper destruction of both paper records and computerized data containing sensitive personal information that could be misused. NAID's mission is to champion the responsible destruction of confidential information and materials by promoting the highest standards and ethics in the industry.

Introduction

Identity theft is a serious crime that imposes enormous costs on society. In its most recent report, the Federal Trade Commission ("FTC") concluded that in 2005 over 8 million U.S. adults were victims of some form of identity theft, with total losses exceeding $15 billion.[2] Identity theft victims face lost job opportunities, loan denials, and huge intangible costs as they devote months and years to rectifying their damaged credit records. Numerous identity theft crimes are

[1] SEC Release No. 34-57427, IC-28178; 1A-2712, 73 Fed. Reg. 13,692 (March 13, 2008) ("Release").
[2] Synovate/FTC Identity Theft Survey Report (November 2007), http://www.ftc. gov/os/ 2007/11/SynovateFinalReportIDTheft2006.pdf.

committed by so-called "dumpster divers" who uncover sensitive financial information after it has been disposed, and use other consumers' account information to make expensive purchases.

One of the most efficient and effective ways to prevent identity theft is to ensure the proper disposal of confidential information at the point when documents are discarded in the normal course of business. It makes far greater sense to adopt a strengthened rule that prevents these "dumpster divers" and other criminals from accessing information, than waiting until after massive losses have occurred and attempting (often unsuccessfully) to find and prosecute the perpetrators after the fact. Not only would the benefits of a strengthened rule in preventing identity theft be high, but the associated costs would be relatively low. A stronger disposal rule would not place undue burdens on broker-dealers and other financial institutions because the practice of shredding confidential documents is a simple, low-cost means to prevent these crimes of opportunity.

To this end, NAID commends the SEC for proposing a strong, balanced, and well-designed expanded disposal rule that will help ensure appropriate disposal of records containing sensitive financial or personal information and thereby prevent identity theft. The Release properly recognizes the public's expectation that when broker-dealers and other financial institutions obtain personal information, it will be handled with care and responsibility.

Requiring secure disposal will not be burdensome for affected firms. In fact, most broker-dealers and other financial institutions are already complying with disposal requirements, and those who are not are obtaining a cost advantage for not taking on the responsibility. Additionally, the size of the entity should not matter for purposes of whether documents are disposed of properly. From the perspective of consumers, the point is that sensitive financial information should be destroyed in a manner that prevents identity theft, regardless of whether a small company or a large company possesses that information. In fact, it may be even more important to require strict compliance from smaller businesses that handle personal information that may not have faced the need in the past to develop disposal policies.

In this regard, NAID supports flexibility with respect to the means of disposal. A reasonableness standard should come into play by allowing certain small firms to use inexpensive shredders to comply with the rule, but it should not relieve them from their obligation to properly dispose of protected information. Another policy reason for mandating proper disposal is that failure to do so can expose financial institutions to significant liability, adverse publicity, and loss of good will. In turn, this could result in a general loss of investor confidence in securities firms.

Our comments below begin with a discussion of the need to establish a standard for what constitutes "proper disposal." This should be a flexible, results-oriented standard that takes into account the varying nature of operations from small to large firms. Next, we support the expanded definition of the information covered by the Release, the imposition of individual liability for violations, and the requirement to maintain written records of disposal. We then address the importance of exercising due diligence in selecting third parties that provide disposal services. Finally, we urge the Commission to treat improper disposal as the functional

equivalent of a security breach requiring notice to individuals whose information may have been compromised.

Addition of "Proper Disposal" Standard

As proposed, the Release does not provide guidance as to what constitutes "proper disposal." The absence of a definition will lead to uncertainly among brokers-dealers and other financial institutions as to what methods of disposal will be considered acceptable by the Commission. Accordingly, NAID proposes that the Commission provide a clear standard along the lines of what is found in the FTC's FCRA disposal rule,[3] In this regard, the Commission should make it clear that throwing personal information into the trash, without ensuring its destruction, would not be sufficient. Instead, NAID believes that adopting a performance standard will provide the best guidance without specifying the procedures to be used in any given situation. NAID recommends the addition of the following standard:

> Personal Information covered by this regulation must be destroyed through shredding, pulverizing, burning, cleansing (in the case of electronic media), or other methods such that it cannot practicably be read or reconstructed. Every broker and dealer other than a notice-registered broker or dealer, every investment company, every investment adviser or transfer agent registered with the Commission, and every natural person who is an associated person of a broker or dealer, a supervised person or a broker or dealer, a supervised person of an investment advisor registered with the Commission, shall implement and take reasonable steps to monitor compliance with policies and procedures that require the proper destruction of Consumer Information, whether contained in hard copy or electronic form, in accordance with this disposal standard.

This modification would provide added protection against identity theft by requiring covered entities to adopt policies and procedures that comport with the rule. A critical component of any "reasonable" document destruction program is to take reasonable steps to ensure that protected documents are being disposed of properly.

Expanded Definition of Personal Information

The Commission implemented the Gramm-Leach-Bliley Act ("GLBA") safeguards requirements and Fair Credit Reporting Act ("FCRA") disposal requirements in Reg. S-P at different times and under different statutes that varied in scope. The Commission now proposes to amend Regulation S-P so that both safeguards and disposal rules will protect all information previously covered by either statute. This new category of information, referred to as "personal information," would include any record containing either non-public personal information or consumer report information. The proposed definition of personal information would include any information identified with any consumer or with any employee, investor, or security holder

[3] 16 C.F.R. § 682.1 et seq.

who is a natural person in paper, electronic or other form that is handled by the institution or maintained on the institution's behalf, including user names and passwords.

NAID strongly supports the expanded scope of coverage of the disposal rule. Financial institutions collect a wealth of information directly from consumers, including Social Security Numbers, dates of birth, mother's maiden name that, if compromised, could be used by an identity thief to establish a new identity. Limiting proper disposal requirements to information from consumer reports would leave unprotected a wealth of sensitive consumer information. Thus, having the safeguards and disposal rules apply to the same categories of information will provide much needed protection.

Even in the absence of the proposed expansion of the disposal rule, it could be argued that a reasonable safeguards program would encompass proper disposal of sensitive information. The goal of safeguarding customer information would not be met if such information was made subject to firewalls, passwords, and restricted access facilities staffed by fully screened personnel, only to be placed unprotected in a dumpster when its useful life was over, thus making it available to anyone willing to dive into a dumpster – something identity thieves are quite willing to do. Thus, it many ways, the Commission is making explicit what should have been implicit in its current safeguard requirements.

The Commission is also to be commended for extending the definition of personal information to employee information. In addition to the identified concern that failure to properly dispose of such information could permit identity thieves to impersonate employees and gain improper access to client information, employees merit protection in their own right. Furthermore, it would be disruptive of company operations, and lead to a lack of confidence in the company, if a failure to protect employee information led its own employees to become victims of identity theft.

Individual Liability for Disposal Violations

The Commission proposes to expand the application of the disposal rules to individuals associated with covered financial institutions. The concern is that such individuals working in remote locations might not properly dispose of information. If the Commission believes that such liability will encourage greater compliance, NAID supports the creation of individual liability.

Supporting the Requirement to Maintain Written Records

As proposed in the Release, broker-dealers would be required to document compliance with safeguards and disposal rules and maintain written records of related policies and procedures. Record retention requirements would be consistent with existing recordkeeping rules. NAID supports the requirement that broker-dealers be required to document compliance with disposal requirements. This will require that compliance mechanisms be established in order to determine how information disposal should be carried out and what type of documentation will be required. The creation of a written record will make clear to internal compliance personnel and the SEC conducting examinations that firms have complied with these disposal provisions.

Prescribing Elements of Due Diligence in Selecting Destruction Contractors

It is likely that many broker-dealers and other financial institutions, both large and small, will outsource their destruction duties to private firms that specialize in information destruction. Accordingly, NAID proposes that the rule be revised to add provisions that require covered entities that outsource their destruction of personal information should in all cases be required to conduct due diligence on the record disposal company, enter into a contract governing the record disposal, and take reasonable steps to monitor performance.

The general duty to conduct an appropriate due diligence analysis already exists in the case of broker-dealers that are members of self-regulatory organizations.[4] NAID believes that the Commission should expand this duty, and apply it to other financial institutions, by prescribing specific elements of due diligence. Such an approach would be consistent with the FTC's "Standards for Safeguarding Customer Information"[5] under Gramm-Leach-Bliley. The FTC rule requires covered entities to "(o)versee service providers, by: (1) Taking reasonable steps to select and retain service providers that are capable of maintaining appropriate safeguards for the customer information at issue; and (2) Requiring your service providers by contract to implement and maintain such safeguards.[6] The Interagency Guidelines Establishing Standards for Safeguarding Information under GLB and the Federal Deposit Insurance Act, which were promulgated by the Comptroller of the Currency,[7] Federal Reserve System,[8] Federal Deposit Insurance Corporation[9] and National Credit Union Administration[10] include similar requirements. These Guidelines require a covered institution to: "(e)xercise appropriate due diligence in selecting its service providers[11] "(r)equire its service providers by contract to implement appropriate measures designed to meet the objectives of these Guidelines[12] and where indicated by institutions' "risk assessment, monitor its service providers to confirm that they have satisfied their obligations. . . . As part of this monitoring, a "bank, bank holding company, or credit union," should review audits , summaries of test results, or other equivalent evaluations of its service providers.[13] The revisions could follow the approach adopted in the FTC's disposal rule:

---

[4] See NASD Notice to Members, 05-48 (July 2005); Proposed NYSE Rule 340 ("Outsourcing: Due Diligence in the Use of Service Providers), File No. SR-NYSE 2005-22 (Amendment No. 2).

[5] 16 C.F.R. § 314.1.

[6] 16 C.F.R. § 314.4(d) (emphasis added).

[7] 12 C.F.R. § 30, App. B § III(D).

[8] 12 C.F.R. § 225, App. F § II(D).

[9] 12 C.F.R. § 364, App. B § III(D).

[10] 12 C.F.R. § 748, App. A § II(D).

[11] 12 C.F.R. § 30, App. B II(D)(I); 12 C.F.R. § 225, App. F § III(D)(I); 12 C.F.R. § 364, App. B III(D)(I); 12 C.F.R. § 748, App. A § III(D)(I). Under these Guidelines service provider" means "any person or entity that maintains, processes, or otherwise is permitted access to customer information through its provision of services directly to the bank, bank holding company, or credit union. 12 C.F.R. § 30, App. B § I(C)(2)(e); 12 R. § 225, App. F § I(C)(2)(e); 12 C. R. § 364 , App. B I(C)(2)(e); 12 C.F.R. 748 App. A § I(B)(2)(d).

[12] 12 C.F.R. § 30, App. B § II(D)(2); 12 C.F.R. 225, App. F § III(D)(2); 12 C.F.R. 364, App. B III(D)(2); 12 C.F.R. § 748, App. A § III(D)(2) (emphasis added).

[13] 12 C. R. § 30, App. B § II(D)(3); 12 C.F.R. § 225, App. F § III(D)(3); 12 C.F. § 364, App. B § III(D)(3); 12 C.F.R. § 748, App. A § II(D)(3). Similarly, under the U.S. Department of Health and Human Services standards for the Health Insurance Portability and Accountability Act ("HIP AA"), a covered entity that permits a business associate to maintain its electronic protected health information must enter a written contract or other written

> After due diligence, entering into and monitoring compliance with a contract with another party engaged in the business of record destruction to dispose of material, specifically identified as consumer information, in a manner consistent with this rule. In this context, due diligence could include reviewing an independent audit of the disposal company's operations and/or its compliance with this rule, obtaining information about the disposal company from several references or other reliable sources, requiring that the disposal company be certified by a recognized trade association or similar third party, reviewing and evaluating the disposal company's information security policies or procedures, or taking other appropriate measures to determine the competency and integrity of the potential disposal company.

FTC Rule, Section 682.3(b)(3).

The preamble to the final rule should explicitly state that these due diligence examples provide a safe harbor whereby broker-dealers and other financial institutions are assured that adopting these practices will satisfy the regulations. When record owners employ methods that are not covered by the examples, they will be proceeding at their own risk. In this way the disposal standard is clear, and the examples clarify that the sample practices that meet this standard.

Improper Disposal as Data Breach

Finally, NAID recommends that the Commission clarify that improper disposal of personal information can constitute unauthorized access to or use of personal information which, in turn, could trigger the obligation to notify individuals of such unauthorized use. Without proper disposal, discarding personal information in the trash can make it easily available to identity thieves. Instead of the more typical breach situation in which a criminal goes through great efforts to obtain access to sensitive information, improper disposal essentially gives this information to the criminal creating just as much potential for mischief and harm. Thus, where misuse of improperly disposed of information has occurred or is reasonably possible, the rule should specify that notice to affected individuals be provided.

* * * * *

Again, we commend the Commission's efforts to enhance the existing information safeguards. The Release provides substantial expanded protections against identity theft. We respectfully request that the SEC consider our proposed clarifications and modifications, which

---

arrangement that documents satisfactory assurances that the business associate will appropriately safeguard the information. 45 C.F.R. § 164. 308(b)(1), (4). In particular, such a contract must provide that the business associate will "(i)mplement administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information" in its possession. 45 C.F.R. § 164. 314(a)(2)(i)(A).

we believe will further serve the laudable goal of minimizing identity theft in an efficient and effective manner.

Respectfully submitted,

Robert Johnson, Executive Director