



National Association for Information Destruction, Inc.

3420 East Shea Blvd., Suite 120, Phoenix, Arizona 85028

Phone: (602) 788-6243 Facsimile: (602) 788-4144

Email: exedir@naidonline.org Website: www.naidonline.org

October 20, 2004

BY ELECTRONIC FILING

Jonathan G. Katz, Secretary
Securities and Exchange Commission
450 Fifth Street, N.W.
Washington, D.C. 20549-0609

RE: Comments on "Disposal of Consumer Report Information,"
File No. S7-33-04

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 regulations entitled, "Disposal of Consumer Report Information."¹ These proposed regulations were drafted pursuant to Section 216 of the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act"), which adds a new section 628 to the Fair Credit Reporting Act ("FCRA").²

Introduction

Identity theft is a serious crime that imposes enormous costs on society. As the preamble recognizes, tens of millions of Americans have been victims of identity theft over a recent five-year period, and this crime has cost businesses, financial institutions, and consumer victims over \$50 billion during a recent year.³ Numerous identity theft crimes are committed by so-called "dumpster divers" who uncover sensitive financial information after it has been discarded, and use other consumers' account information to make expensive purchases.

The Commission has requested comment on the potential costs and benefits associated with its proposal. One of the most efficient and effective ways to prevent identity theft is to ensure the destruction of confidential information at the point when documents are discarded in the normal course of business. It makes far greater sense to adopt a strong rule that prevents these "dumpster divers" and other criminals from accessing information, than waiting until after massive losses have occurred and

¹ Disposal of Consumer Report Information, 69 Fed. Reg. 56304 (Sept. 20, 2004) (to be codified at 17 C.F.R. pt. 248).

² 15 U.S.C. § 1681.

³ 69 Fed. Reg. at 56308.

attempting (often unsuccessfully) to find and prosecute the perpetrators after the fact. Not only are the benefits of a strong rule preventing identity theft high, but the associated costs are relatively low. A strong disposal rule would not place undue burdens on financial institutions because the practice of shredding confidential documents is a simple, low-cost means to prevent these crimes of opportunity.

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 members are on the front lines of the information disposal work that is addressed by this rule, and NAID commends the SEC for setting forth a strong, balanced, and well-designed rule that will help ensure appropriate disposal of records containing sensitive financial or personal information and thereby prevent identity theft. The proposed rule recognizes the public's right to expect that when financial institutions obtain consumer report information, it will be handled with care and responsibility. As set forth below, NAID recommends that the Commission clarify a handful of issues and further bolster the rule in several respects. NAID's comments are principally focused on ensuring that the rule is effective in preventing identity theft and that it cannot be easily circumvented.

These comments begin with a discussion of the reasonableness standard and, in particular, the preamble's description and examples of reasonable practices. Within this discussion, we respond to the SEC's proposed revision to its safeguard rule which would specify that covered entities must state in writing their safeguard policies and procedures. Second, we comment on the proposed definition of "consumer report information." Third, we discuss the proposed definition of "disposal," and the proper disposal of information stored electronically. Fourth, we address the scope of the proposed rule and, finally, we comment on the SEC's statement regarding other legal authority that may be relevant to the requirements stated in this rule.

A. Reasonableness Standard

In general, the proposed rule strikes the right balance between setting strict standards to prevent identity theft and protecting financial institutions from undue burdens. A reasonableness standard provides appropriate flexibility, which permits small institutions to use inexpensive methods of disposal, while requiring certain larger institutions to do more to ensure proper disposal of the volumes of "consumer report information" they utilize.

1. Commentary

Although NAID supports a reasonableness standard, the SEC's preamble to the proposed rule contains some descriptions of "reasonable" practices that are not consistent with the statutory mandate to increase protections against identity theft. In particular, the commentary states: "In determining what measures are 'reasonable' under the proposed disposal rule, we expect that entities covered by the rule would consider the sensitivity of the consumer report information, the size of the entity and the complexity of its operations, the costs and benefits of different disposal methods, and relevant

technological changes."⁴ To the extent this commentary suggests that costs, evolving technologies, and the sophistication of the financial institution might affect the reasonableness of the disposal method it employs—*e.g.*, a large, sophisticated company might use the state-of-the-art technology for "wiping" computer hard drives, while a small company might simply remove and smash a hard drive before disposing of a computer—we agree. On the other hand, to the extent this language suggests that financial institutions might treat different types of consumer report information differently—based on the company's own assessment of the "sensitivity" of that information—we disagree. In passing the FACT Act, Congress made a clear judgment regarding what categories of information should be covered and decided that *all* information in or derived from consumer reports is sufficiently sensitive to require proper disposal.⁵ Reasonableness cannot mean that entities will be immune from federal law when they fail properly to dispose of *any* protected consumer report information. Similarly, the rule should clarify that it is *never* reasonable for financial institutions to fail to destroy records at the time of disposal when consumer report information is contained within those records—even when they possess only a small amount of this information. Given the danger posed by dumpster divers, it is critical that the rule cover *all* consumer report information.

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 institution or a large institution possesses that information. It is also clear that small entities do not require a special set of rules to avoid an undue burden. As the Better Business Bureau has recognized, "[e]ven the smallest business can afford an inexpensive paper shredder."⁶ Accordingly, NAID supports flexibility with respect to the means of disposal, but the information covered and the resulting destruction must comport with Congress' mandate. In other words, the reasonableness standard should come into play by allowing certain small institutions to use inexpensive shredders or similar methods to comply with the rule, but it should not relieve them from their obligation properly to dispose of protected information.

2. Examples of Reasonableness

The SEC seeks comment on the proposed standard for disposal, and specifically questions whether the proposed disposal rule should provide specific examples. The SEC's commentary sets forth three examples of reasonable disposal measures,⁷ and

⁴ 69 Fed. Reg. at 56306.

⁵ FACT Act § 216(a), 117 Stat. at 1985 (adding FCRA § 628(a)(1)) (to be codified at 15 U.S.C. § 1681w).

⁶ Better Business Bureau, *Information for Businesses - In the Real World*, at <http://www.bbbonline.org/idtheft/business.asp>.

⁷ 69 Fed. Reg. at 56306-7.

NAID commends the SEC on the substance of these examples. Indeed, NAID strongly believes that, to the extent they are applicable in a given context, the measures described in each example should be stated as rule requirements and not merely optional compliance methods. This revision would provide helpful guidance to covered entities, and leave them with more certainty about whether they are complying with the rules.

a) **Disposal Standard**

The first and second examples state, respectively, that reasonable measures of disposal would include "[i]mplementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers" and "the destruction or erasure of electronic media" such that "*the information cannot practicably be read or reconstructed*."⁸ The language specifying that proper disposal requires destruction such that "the information cannot practicably be read or reconstructed"⁹ is central to the proposed rule and, accordingly, should be incorporated in the text of the rule itself. It strikes the right balance between achieving Congress' goal of reducing the incidence of identity theft resulting from improper disposal of records without imposing unreasonable burdens in the process. Without this clarification, the rule would fail to provide a clear standard with respect to the core issue presented and might invite controversy and uncertainty as to whether it remains permissible, at least in some cases, merely to throw consumer report information into the trash without ensuring its destruction.

Accordingly, we recommend adding the following sentence to the end of the standard provision, proposed section 248.30(b)(2)(i):

Information covered by this regulation must be destroyed through shredding, pulverizing, burning, destruction or erasure (in the case of electronic media), or other methods such that it cannot practicably be read or reconstructed.

With respect to the remaining language in the first two examples, we recommend combining and enhancing these ideas into one requirement that states:

Covered entities shall implement and take reasonable steps to monitor compliance with *written* policies and procedures that require the proper destruction of consumer report information, whether contained in hard copy or electronic form, in accordance with the disposal standard stated in Section 248.30(b)(2)(i).

These mandates are critical components of any "reasonable" document destruction program, they will provide added protection against identity theft, and they will meet the Commission's goal of "maintain[ing] a flexible approach, while establishing certain

⁸ 69 Fed. Reg. at 56307 (emphasis added).

⁹ *Id.*

elements in the rule that a firm must include in its policies and procedures."¹⁰ In addition to this formulation of the rule, NAID supports the SEC's statement in the commentary that "[r]easonable measures' may require elements such as the establishment of policies and procedures governing disposal, as well as appropriate employee training."¹¹

Moreover, for the same reasons that the SEC proposes to amend its safeguard rule to specify that covered entities must state in writing their safeguard policies and procedures,¹² the disposal rule should do the same. NAID shares the SEC's assessment that, absent written policies and procedures, it is difficult for firms effectively to safeguard consumer report information, and it is also difficult to evaluate compliance with the safeguard rule.¹³ Accordingly, in answer to the SEC's requests for comments on whether the safeguard rule and the disposal rule should require written policies and procedures, NAID endorses such requirements for both rules.

b) **Due Diligence Requirement**

The third example of a reasonable disposal measure listed in the commentary is: "After due diligence, entering into and monitoring compliance with a written contract with another party engaged in the business of record destruction to dispose of consumer report information in a manner that is consistent with this rule."¹⁴ NAID proposes that financial institutions who outsource their destruction of consumer report 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.

We suggest a new provision titled, "Due Diligence Requirements," that states:

All covered entities who contract with third parties to destroy consumer report information shall conduct due diligence on the record disposal company, enter into a written contract governing proper record disposal, and take reasonable steps to monitor contract compliance.

Following this section, we recommend that the SEC insert its examples of due diligence, along with one additional example of disposal companies destroying materials according to a published standard that is similar to the criteria applied by reputable certifying agencies. In this way, the examples would incorporate flexibility relating to due

¹⁰ 69 Fed. Reg. at 56308.

¹¹ 69 Fed. Reg. at 56306.

¹² 69 Fed. Reg. at 56307-8.

¹³ *Id.*

¹⁴ 69 Fed. Reg. at 56307.

diligence, while articulating the need for those engaged in document destruction to meet generally accepted standards. Accordingly, we propose the following language:

Examples. 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, ensuring that the disposal company destroy the materials according to a published standard that is similar to the criteria applied by reputable certifying agencies, 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.

Finally, the commentary on the rule should explicitly state that these due diligence examples provide a safe harbor whereby financial institutions are assured that adopting these practices will satisfy the regulations. When financial institutions employ methods that are not covered by the examples, they will be proceeding at their own risk. In this way, the examples would further clarify which practices would meet the FACTA standard.

B. "Consumer Report Information"

The Commission defines "consumer report information" as "any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report,"¹⁵ and requests comment on this proposed definition. The commentary explains that "information that is derived from consumer reports but does not identify any particular individual would not be covered under the proposed rule."¹⁶ Although NAID does not disagree with this statement, it is essential that the Commission clarify that the term "identify" includes all information that may allow an identity thief to associate the relevant information with a particular person. In reality, addresses, telephone numbers, social security numbers, and other pieces of information can be used to identify individuals with little effort, and this information should be encompassed within the meaning of "identify." NAID specifically recommends that the Commission should exempt from its definition of "consumer report information" only information that *could not* be used to identify individuals. Such a narrow exemption is consistent with the Commission's recognition that "[a] broad definition of [consumer report information] . . . may best effectuate the purposes of the FACT Act."¹⁷

¹⁵ Proposed Section 248.30(b)(1)(ii).

¹⁶ 69 Fed. Reg. at 56305.

¹⁷ *Id.*

In further response to the Commission's request for comment with respect to the scope of the information covered by the proposed rule, NAID addresses the Commission's assessment that the disposal rule applies to the "customer records and information" subject to the safeguard rule under the Gramm-Leach-Bliley Act ("GLBA") *to the extent that* such documents overlap with "consumer report information" subject to the proposed disposal rule.¹⁸ NAID recommends that the SEC direct that the disposal rule standards should apply to *all* material covered by the GLBA and not just to material that qualifies as consumer report information. In other words, all entities subject to the safeguard rule should follow the same standards articulated in the disposal rule when disposing of information covered by the GLBA. This recommendation is consistent with the GLBA's fundamental statement of Congress' policy "that each financial institution has an affirmative and continuing obligation to respect the privacy of its customers and to protect the security and confidentiality of those customers' nonpublic personal information."¹⁹ Additionally, NAID's proposed formulation would remove doubt regarding what information is covered by the rules governing information security, and would avoid the complexity of applying different disposal rules to different classes of information. Such a clear rule also would eliminate the need for record holders to parse through documents to identify covered information.

C. "Disposal"

The Commission seeks comment on the proposed definition of the term "disposal." For the most part, NAID supports the SEC's definition. NAID, however, recommends replacing the word "and" with the word "or" at the end of the first part, in order to clarify that each of the two parts independently constitutes "disposal." We also suggest that the term "discarding" be incorporated within section (2) of the definition.

In many situations, there will be transfers of computer equipment from one entity to another that are not intended to constitute an effort to discard information, such as when computers are transferred from one corporate affiliate to another.²⁰ This situation differs from an example in the commentary, which states: "If the entity donates computer equipment on which consumer report information is stored, however, the donation would be considered a disposal under the proposal."²¹ NAID recommends that the definition of "disposal" should incorporate an intent requirement to clarify the distinction between the sale, donation, or transfer of computer equipment where (a) there is no intent to transfer the information but only the equipment versus (b) there is an intent to transfer the information as part of the transaction. The summary of the proposed rule explains: "The sale, donation, or transfer, as opposed to the discarding or abandonment, of consumer

¹⁸ 69 Fed. Reg. at 56306.

¹⁹ 15 U.S.C. 6801(a).

²⁰ This presumes a legal right to transfer consumer report information from one affiliate to another under FCRA or other applicable laws.

²¹ 69 Fed. Reg. at 56305.

report information would not be considered a 'disposal' under the proposed Rule."²² Incorporating an intent requirement into the definition of "disposal" would clarify this distinction. Accordingly, we suggest the following language:

***Disposal* means: (1) The discarding or abandonment of consumer report information, or (2) The sale, donation, transfer, or discarding of any medium, including computer equipment, on which consumer report information is stored, absent a good faith intent to transfer such consumer report information to a third party for legitimate business purposes.**

D. Scope of Covered Entities

The Commission seeks comment on the scope of the proposed rule. NAID does not think that "there are any 'persons or classes of persons' covered by the proposed disposal rule that [the Commission] should consider exempting from the rule's application."²³ Because the cost of compliance with the disposal rule is low, because the benefits are very high, and because any loophole would both undermine the purpose of the law and would risk preventable identity theft, NAID encourages the SEC to reject any proposals for exemptions.

NAID notes that potential misunderstandings may arise from the SEC's explanation of why it is not covering notice-registered broker-dealers and, in particular, the statement that these broker-dealers "are subject to primary oversight by the [Commodity Futures Trading Commission] and are exempted from all but the core provisions of the laws administered by the Commission."²⁴ To the extent that notice-registered broker-dealers are not covered by the SEC, they are covered by the FTC's residual jurisdiction under the FCRA. As the commentary explains: "'Section 621 of the [FCRA] grants enforcement authority to the FTC for all persons subject to the FCRA 'except to the extent that enforcement * * * is specifically committed to some other government agency under subsection (b)' of section 621. 15 U.S.C. 1681s."²⁵ To prevent the misimpression that notice-registered broker-dealers are exempt from the FACT Act because they are not subject to the SEC's jurisdiction, NAID recommends that the SEC clarify that these broker-dealers are subject to the FTC's enforcement authority.

E. Related Legal Authority

Finally, the Commission seeks comment on "the extent to which other federal standards involving privacy or security of information may duplicate, satisfy, or inform

²² *Id.*

²³ 69 Fed. Reg. at 56306.

²⁴ 69 Fed. Reg. at 56307, n.25.

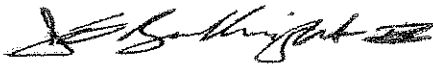
²⁵ *Id.* at n.23.

the proposal's requirements," in addition to comment "about any statutes or rules that may conflict with the proposed disposal rule requirements, as well as any other state, local, or industry rules or policies that require covered entities to implement practices that comport with the requirements of the proposed rule."²⁶ Consistent with the Commission's assessment, NAID is not aware of any authority "that would conflict with the proposed disposal rule's requirement (i) that covered persons take reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal or (ii) that safeguarding policies and procedures must be in writing."²⁷ Moreover, to the extent that the provisions of the GLBA overlap in part with the disposal rule, we do not believe that the current safeguard policies satisfy the requirements of the FACT Act.

* * * * *

Again, we commend the proposed regulations, as they provide substantial new protections against identity theft and further Congress' purpose in enacting the FACT Act. We respectfully request that the SEC consider our proposed clarifications and modifications, which we believe will further serve the laudable goal of minimizing identity theft in an efficient and effective manner.

Respectfully submitted,



John Bauknight IV, President



Robert Johnson, Executive Director

²⁶ 69 Fed. Reg. at 56312.

²⁷ *Id.*