Comment #: 49

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

June 15, 2004

BY ELECTRONIC FILING
Federal Trade Commission
Office of the Secretary
Room 159-H (Annex H)
600 Pennsylvania Avenue, N.W.
Washington, D.C. 20580

RE: Comments on "The FACT Act Disposal Rule, R-411007"

To the Commission:

The National Association for Information Destruction, Inc. ("NAID") submits these comments on the Federal Trade Commission's ("FTC" or "Commission") proposed regulations entitled, "Disposal of Consumer Report Information and Records,"[1] which were drafted pursuant to Section 216 of the Fair and Accurate Credit Transactions Act of 2003 ("FACT Act").

Introduction

Identity theft is a serious crime that imposes enormous costs on society. As the FTC has documented, tens of millions of Americans have been victims of identity theft, costing consumers and businesses tens of billions of dollars.[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 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 strong 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 strong

---

1 69 Fed. Reg. 21388 (Apr. 20, 2004) (to be codified at 16 C.F.R. pt. 682).

2 Synovate/FTC, Identity Theft Survey Report 6-7 (Sept. 2003), *at* http://www.ftc.gov/os/ 2003/09/synovatereport.pdf; *see also*, Report: Overview of the Identity Theft Program (Oct. 1998 – Sept. 2003) (Sept. 2003), *at* http://www.ftc.gov/os/2003/09/timelinereport.pdf.

rule in preventing identity theft be high, but the associated costs would be relatively low. A strong disposal rule would not place undue burdens on covered entities 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. We are on the front lines of the information disposal work that is addressed by this rule. We commend the FTC 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 businesses obtain consumer 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. It is particularly important that the FTC adopt strict standards because this rule will preempt certain state laws that require proper disposal of the same information covered by the FACT Act[3] and it certainly was not Congress' intent to weaken current identity theft protections.[4]

These comments begin with a discussion of the reasonableness standard. In particular, we address the description of reasonable practices in the preamble and the examples listed in the rule, including the examples pertaining to the disposal standard and outsourcing. Second, we discuss the issue of custodian liability, including the appropriate allocation of duties in the outsourcing context and the proposed exemption for traditional garbage collectors. Third, we propose language to ensure clear standards, and address the relationship of this rule with Gramm-Leach-Bliley ("GLB"). Fourth, we discuss the definitions of "consumer information" and "business purposes," and the proper disposal of information stored electronically. Finally, we have attached a new version of the rule which reflects these comments.

A. Reasonableness Standard

In general, the proposed rule strikes the right balance between setting strict standards to prevent identity theft and protecting record owners from undue burdens. A

---

[3] The FACT Act amends the Fair Credit Reporting Act's ("FCRA") preemption provision. This amended provision states: "No requirement or prohibition may be imposed under the laws of any State . . . with respect to the conduct required by the specific provisions of . . . section 628." FACT Act § 711(2), 117 Stat. 1952, 2011 (2003) (to be codified at 15 U.S.C. § 1681t(b)). In turn, Section 628 governs "Disposal of Records."

[4] At present, at least three states—Georgia, California, and Washington—have enacted disposal laws. *See* Ga. Code Ann. §§ 10-15-1, 10-15-2, 10-15-6; Cal. Civ. Code § 1798.81; Wash. Rev. Code ch. 19.215.

reasonableness standard provides appropriate flexibility, which permits small businesses to use inexpensive methods of disposal, while requiring certain larger businesses to do more to ensure proper disposal of the volumes of "Consumer Information"[5] they utilize. As the Better Business Bureau has recognized, "[e]ven the smallest business can afford an inexpensive paper shredder."[6]

1. Commentary

Although NAID supports a reasonableness standard, the FTC'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 Rule, the Commission expects that entities covered by the proposed Rule would consider the sensitivity of the consumer information, the nature and size of the entity's operations, the costs and benefits of different disposal methods, and relevant technological changes."[7] It makes sense to consider both the costs and benefits of different disposal *methods* and the evolving technology but not the sensitivity of the Consumer Information. In passing the FACT Act, Congress has already made the calculus on the nature of covered information by deciding that *all* information in or derived from consumer reports is sufficiently sensitive to require proper disposal.[8] Reasonableness cannot mean that entities will be immune from federal law when they decide that it is not important properly to dispose of *any* protected Consumer Information. Similarly, the rule should clarify that it is *never* reasonable for record owners to use standard garbage disposal methods when they have reason to know that Consumer Information is contained within their records, even when they possess only a small amount of this information. Given the tenacity of some dumpster divers, it is critical that the rule cover *all* Consumer 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 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 Consumer Information that may not have faced the need in

---

5 "Consumer Information" is a defined term in the proposed rule. Proposed Section 682.1(b). As discussed below, NAID suggests a revised definition such that the term means "all records and files of information about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report." *See infra*, at 11. Throughout these comments, NAID's references to "Consumer Information" refer to this revised definition.

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

7 69 Fed. Reg. at 21389.

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

the past to develop disposal policies. For example, a small car dealership that improperly disposes of consumer reports obtained to consider financing requests could be a significant source of information for an identity thief. 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 businesses to use inexpensive shredders to comply with the rule, but it should not relieve them from their obligation to properly dispose of protected information.

2. Examples of Reasonableness

The proposed rule sets forth four examples of "[r]easonable measures to protect against unauthorized access to or use of consumer information in connection with its disposal."[9] NAID commends the FTC on the substance of these examples. In fact, 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.

a) Disposal Standard

Examples #1 and #2 state 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.*"[10] The language which defines proper disposal as destruction such that "the information cannot practicably be read or reconstructed"[11] should be incorporated in the general standard. 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 central issue presented and might invite controversy and uncertainty as to whether it remains permissible, at least in some cases, merely to throw Consumer Information into the trash without ensuring its destruction.

Here, it is important to note that the Washington state statute, "Disposal of Personal Information," mandates: "An entity must take all reasonable steps to destroy, or arrange for the destruction of, personal financial and health information and personal identification numbers issued by government entities in an individual's records within its custody or control when the entity is disposing of records that it will no longer retain."[12] The statute, in turn, defines "[d]estroy personal information" as "shredding, erasing, or otherwise modifying personal information in records to make the personal information

---

9 Proposed Section 682.3(b).

10 Proposed Sections 682.3(b)(1)-(2) (emphasis added).

11 *Id.*

12 Wash. Rev. Code § 19.215.020(1).

unreadable or undecipherable through any reasonable means."[13] The approach adopted by the State of Washington is both fair and effective, and we encourage the Commission to adopt a similar approach here. Indeed, because the FTC rule will preempt certain application of the Washington statute, it is all the more important for the FTC to incorporate a strong, clear standard of destruction.

Accordingly, we recommend adding the following sentence to the end of the standard provision, § 682.3(a):

> **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.**

With respect to the remaining language in Examples #1 and #2, we recommend combining the ideas into one requirement which states:

> **Covered entities 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 the disposal standard stated in Section 682.3.**

This modification will 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 monitor compliance to insure that protected documents are being disposed of properly.

It may prove difficult to apply the disposal standard when computer equipment containing protected information is the subject of a transfer. There is a risk that Consumer Information could be retrieved from transferred computer equipment and used to commit identity theft. However, the information wiping software that is available today generally cannot, without effectively destroying the computer's memory, so completely destroy electronically stored data that the data is rendered irretrievable, even with the most sophisticated technology.[14] Yet, a standard requiring hardware destruction would impede the donation of computer equipment to schools, non-profits and other organizations that would benefit from their use. In order to design an effective and practical rule, the FTC should weigh these competing concerns. Moreover, given the rapid evolution of technology in this area, it will be important for the FTC to address this difficult, unsettled issue on an ongoing basis. The FTC may wish to consider whether standards exist, such as those recommended by the Department of Defense, that would

---

13 Wash. Rev. Code § 19.215.010(2) (emphasis added).

14 *See, e.g.*, Simson L. Garfinkel & Abhi Shelat, *Remembrance of Data Passed: A Study of Disk Sanitization Practices*, 1 IEEE Security & Privacy 17 (Jan./Feb. 2003) ("Garfinkel & Shelat").

appropriately strike the balance between reasonable destruction efforts and preserving valuable corporate computer donation programs. At a minimum, the FTC should specify that, as with paper records, electronic data should be destroyed such that it cannot practicably be read or reconstructed.

b) **Outsourcing Requirements**

Example #3 states that a reasonable measure of disposal would include: "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 information in a manner consistent with this rule."[15] NAID proposes that covered entities who outsource their destruction of Consumer 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.

This proposal for outsourcing requirements is consistent with the FTC's "Standards for Safeguarding Customer Information" 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."[16] 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,[17] Federal Reserve System,[18] Federal Deposit Insurance Corporation,[19] and National Credit Union Administration,[20] include similar requirements. These Guidelines require a covered institution to: "[e]xercise appropriate due diligence in selecting its service providers";[21] "[r]equire its service providers *by contract* to implement appropriate measures designed to meet the objectives of these Guidelines";[22] and

---

15 Proposed Section 682.3(b)(3).

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

17 12 C.F.R. § 30, App. B § III(D).

18 12 C.F.R. § 225, App. F § III(D).

19 12 C.F.R. § 364, App. B § III(D).

20 12 C.F.R. § 748, App. A §III(D).

21 12 C.F.R. § 30, App. B § III(D)(1); 12 C.F.R. § 225, App. F § III(D)(1); 12 C.F.R. § 364, App. B § III(D)(1); 12 C.F.R. § 748, App. A § III(D)(1). 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 C.F.R. § 225, App. F § I(C)(2)(e); 12 C.F.R. § 364, App. B § I(C)(2)(e); 12 C.F.R. § 748, App. A § I(B)(2)(d).

22 12 C.F.R. § 30, App. B § III(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).

"[w]here indicated by the" bank's, bankholding company's, or credit union's "risk assessment, *monitor* its service providers to confirm that they have satisfied their obligations . . . . As part of this monitoring, a" bank, bankholding company, or credit union, "should review audits, summaries of test results, or other equivalent evaluations of its service providers."[23]

Based on this precedent for mandating the type of conduct listed in the outsourcing example, we suggest a new provision within Section 682.3 titled, "Outsourcing Requirements," which states:

> **All covered persons who outsource the destruction of Consumer Information shall conduct due diligence on the record disposal company, enter into a contract governing proper record disposal, and take reasonable steps to monitor contract compliance.**

Following this section, we recommend that the FTC 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 diligence, while articulating the need for those engaged in document destruction to meet generally accepted standards. As such, 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, *requiring 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.**

---

[23] 12 C.F.R. § 30, App. B § III(D)(3); 12 C.F.R. § 225, App. F § III(D)(3); 12 C.F.R. § 364, App. B § III(D)(3); 12 C.F.R. § 748, App. A § III(D)(3). Similarly, under the U.S. Department of Health and Human Services standards for the Health Insurance Portability and Accountability Act ("HIPAA"), a covered entity that permits a business associate to maintain its electronic protected health information must enter a written contract or other written 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).

Finally, the commentary on the rule should explicitly state that these due diligence examples provide a safe harbor whereby record owners 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.

3. Custodian Liability

a) Allocation of Duties

For the most part, third parties such as garbage disposal, recycling, and records storage companies merely act under the direction of record owners, and they have no basis for knowing whether documents in their possession are covered by the rule. Yet, the scope of the proposed rule covers "any person over which the Federal Trade Commission has jurisdiction, that, for a business purpose, *maintains or otherwise possesses* consumer information or any compilation of consumer information."[24] The commentary specifies that "[c]ompanies that possess consumer information in connection with the provision of services to another entity are also directly covered by the proposed Rule *to the extent that they dispose of the consumer information.*"[25] Accordingly, the terms of custodian liability require additional clarification in order to ensure that the rule is fair, practical, and effective and does not impose burdens on firms that have no reason to know they are handling protected information.

The rule should expressly state that third parties are not required to make independent determinations about whether the documents in their custody constitute covered information. Any contrary rule that requires custodians to evaluate the contents of another party's documents would be costly and counter-productive. Clearly, record owners are in the best position to determine whether their records contain Consumer Information. If both record owners and custodians face this duty, custodians would need to hire additional employees to do duplicative work, and the cost of record storage will rise -- dramatically in some cases. And, even if third parties were prepared to conduct such laborious reviews of confidential information, their ability to comply with the rule is doubtful at best. Many third parties are contractually prohibited from examining documents that could contain legally protected or other sensitive information. And even

---

[24] Proposed Section 682.2(b) (emphasis added). NAID commends the FTC on its guidance that "for a business purpose" should read "broadly to include all business reasons for which a person may possess or maintain consumer information. Thus, the Rule would likely cover any person that possesses or maintains consumer information other than an individual who has obtained his or her own consumer report." 69 Fed. Reg. at 21389. Sensitive financial information is readily available to scores of businesses through their receipt of consumer reports. It is critical that "business purpose" be construed broadly, as the FTC articulates, in order to prevent the misuse of this information.

[25] 69 Fed. Reg. at 21389 (emphasis added).

when access is permitted, they simply lack the institutional knowledge required accurately to determine whether financial information was derived from consumer reports. Finally, requiring additional third party review of documents could undermine federal statutes including the Fair Credit Reporting Act, the FACT Act, GLB, and HIPAA, which seek to limit, not increase, access to sensitive financial and health information in order to prevent misuse.

Notwithstanding these issues, we agree with other submitted comments which recognize that third parties who affirmatively take on the responsibility of disposing Consumer Information should be required to do this work in accordance with the FACT Act and applicable federal regulations. Accordingly, we suggest that third parties, including NAID members, should assume the legal duty to comply with the rule after two prerequisites are met: (1) The record owner notifies the third party that documents transferred to the third party contain Consumer Information, and (2) the third party enters a written contract to shred, pulverize or burn documents or to cleanse[26] or destroy electronic media. If these prerequisites are met, it makes sense to allow document owners to shift their obligations to a third party such that one clearly identifiable party bears responsibility for proper disposal at any given time.

However, it would be impractical, inefficient, and unduly burdensome for record custodians to assume liability when these prerequisites are not met. For instance, imposing liability on custodians absent their agreement to destroy records would create perverse incentives for record owners. In particular, record owners may attempt to shift the burden of destroying documents to their custodians without compensation, which would generate controversy—and perhaps litigation—regarding who bears the responsibility for destruction.

b) **Clarification of Garbage Collection Provisions**

For the reasons just discussed, garbage collectors have neither the training nor the resources to assess whether the trash they pick up contains Consumer Information. In attempting to address this concern, the proposed rule currently provides: "For traditional garbage collectors engaged in the normal course of business," an example of a reasonable disposal method is, "disposing of garbage in accordance with standard procedures."[27] However, this example is ambiguous. If it were construed to allow record owners to dispose of Consumer Information through the process of traditional garbage collection, it would eviscerate the proposed rule. Accordingly, it is important to clarify that this is *not* what the rule says. Rather, the rule simply and sensibly exempts traditional garbage collectors from heightened standards regarding waste disposal in order to shield them from the impossible burden of analyzing the contents of the trash they collect. Since the same rationale applies to recycling companies and records management companies, they should be included within this exemption as well.

---

[26] NAID suggests the term "cleanse," instead of "erase," here because current technology overwrites electronic data, and full erasure generally is not possible. *See* Garfinkel & Shelat, *supra* n.14.

[27] Proposed Section 682.3(b)(4)(b).

In order to incorporate this exemption and implement the custodian liability structure addressed above, we suggest reformulating Example #4 by creating a new sub-section (c) under Section 682.3, titled, "Third Party Servicers." This new sub-section should state:

> (1) **Third parties, including garbage collectors, recyclers, or records management and storage companies, are not required to make independent determinations about whether the documents in their custody constitute Consumer Information. Such third parties engaged in the normal course of business are exempt from this rule unless and until the following two conditions are met: (A) The record owner notifies the third party that documents transferred to the third party contain Consumer Information, and (B) the third party enters a written contract with the record owner to dispose of Consumer Information pursuant to the requirements of this rule.**
>
> (2) **Third parties who are not exempt from this rule based on the criteria set forth in Section 682.3(d)(i) shall (A) implement and take reasonable steps to monitor compliance with policies and procedures that protect against unauthorized access to or use of Consumer Information during collection and transportation and (B) dispose of such information in accordance with the standards and requirements of this rule.**

These suggested modifications will close potential loopholes by requiring record owners to arrange for the proper disposal of Consumer Information and requiring third parties who carry out this work to comply with the requisite standards. Record owners will benefit from a justified safe harbor when, after conducting due diligence, they enter a contract for record destruction which specifies that the destruction should be completed in accordance with these rules, and they take reasonable steps to monitor compliance. At the same time, third parties will receive clear notice of their legal duties because their contract obligations will trigger statutory obligations. This notice is of critical importance given the substantial penalties that may be imposed, and liability that may arise, where violations occur.[28] And, most importantly, under our proposal, at all times a clearly identifiable individual or company will bear undisputed responsibility for ensuring compliance with this rule, and that individual or company will not be able to point the finger at some third party.

4. Clear Standards

In addition to these suggestions for comprehensive coverage, NAID recommends a new provision that will advance the dual goals of increasing the effectiveness of the rule in preventing identity theft, and providing clear guidance to covered entities who seek certainty regarding their compliance. The FTC should expressly advise record owners to adopt a policy of shredding *all* documents that could possibly contain

---

[28] *See* 15 U.S.C. § 1681s(a)(2)(A); *see also*, 15 U.S.C. §§ 1681n-1681o.

Consumer Information. This practical advice is especially important when it is not clear what sensitive information is derived from consumer reports. At a minimum, NAID encourages the FTC to disseminate this advice during its business education campaign associated with the promulgation of these regulations.

5. Interplay Between Disposal Rule and GLB Safeguards Rule

Our final point with respect to the reasonableness standard is that the FTC's commentary appropriately recognizes that "a 'reasonable measures' standard would harmonize the Disposal Rule with the Commission's Safeguards Rule, 16 C.F.R. part 314, implementing section 501(b) of the GLBA, so that entities subject to both rules will not face conflicting requirements."[29] Indeed, since GLB and the FACT Act set forth complimentary provisions to achieve the same goals, the guidance appropriate under GLB should apply to the FACT Act, and vice versa. Accordingly, the final rule should expressly state that, to the extent that GLB requires proper disposal of information, the Disposal Rule sets forth the requisite standards under GLB.

B. "Consumer Information"

The proposed rule defines "consumer 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."[30] The rule would be more effective in deterring identity theft if this definition expressly covered the entire file of information that contains a consumer report or information derived from a consumer report. Such a formulation is consistent with the summary of the proposed rule, which explains the Commission's belief that "a broad definition of [consumer information] . . . will best effectuate the purposes of the Act"[31] and that the phrase "derived from consumer reports" includes "information from a consumer report that has been combined with other types of information."[32] Accordingly, in order to prevent gaps in coverage, NAID proposes the following definition of "Consumer Information":

> **All records *and files of information about an individual*, whether in paper, electronic, or other form, that contain a consumer report or information derived from a consumer report.**

Considering the difficulty that record owners and adjudicatory bodies will face when they attempt to discern which information within a file was derived from a consumer report, it makes sense to adopt this bright-line requirement, which incorporates the intent expressed in the FTC's summary. Moreover, NAID recommends clarifying that

---

29 69 Fed. Reg. at 21390.

30 Proposed Section 682.1(b).

31 69 Fed. Reg. at 21389.

32 *Id.*

information "*derived from* a consumer report"[33] includes all information *in whole or in part* based on a consumer report. This clarification will foster compliance under the rule, and promote the purpose of the rule by preventing identity theft.

C. "Business Purpose"

The FACT Act requires the FTC to "issue final regulations requiring any person that maintains or otherwise possesses consumer information, or any compilation of consumer information, derived from consumer reports for a business purpose to properly dispose of any such information or compilation."[34] As an amendment to the FCRA, "any person" refers to the definition of "person" in the FCRA[35] which includes, among other things, governmental entities.[36] Thus, when applied in this context, deriving information from consumer reports for a "business purpose" would include the business of government. It would help place governmental entities on notice that they will be covered by these requirements if the FTC's final rule made clear that information obtained for a "business purpose" includes information obtained from consumer reports to consider consumers' eligibility for government licenses or benefits, government employment, or for other governmental purposes. Accordingly, NAID proposes the following definition of "business purpose" be added to the rule:

> **As used in this part, "business purpose" includes the business of government.**

D. Information Stored Electronically

In the definition of "disposing" or "disposal," NAID 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 "disposing" or "disposal." We also suggest that the term "discarding" be incorporated within section (2) of the definition, as recommended in the comments submitted by Consumers Union. Accordingly, we suggest the following language:

> **As used in this part, "disposing" or "disposal" includes: (1) the discarding or abandonment of Consumer Information, or (2) the sale, donation, transfer, or discarding of any medium, including computer equipment, upon which Consumer Information is stored.**

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

---

33 Proposed Section 682.1(b) (emphasis added).

34 117 Stat at 1985 (adding FCRA § 628(a)(1)) (to be codified at 15 U.S.C. § 1681w).

35 Proposed Section 682.1(a).

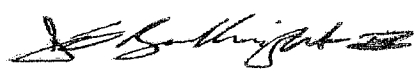
36 15 U.S.C. § 1681a(b).

when computers are transferred from one corporate affiliate to another.[37] Thus, the definition of "disposing" or "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) the information contained on the computer is intended to be part of the transfer. The summary of the proposed rule explains: "By itself, the sale, donation, or transfer of consumer information would not be considered 'disposal' under the proposed Rule."[38] Incorporating an intent requirement into the definition of "disposing" and "disposal" would clarify that this exemption applies to the latter situation, but not the former.

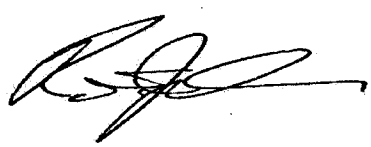
* * * * *

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 FTC 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

---

37 This presumes a legal right to transfer Consumer Information from one affiliate to another under FCRA or other applicable laws.

38 69 Fed. Reg. at 21389.

Language Suggested by NAID for the FTC Rule:
"Disposal of Consumer Report Information and Records"

§ 682.1 Definitions

(a) *In general.* Except as modified by this part or unless the context otherwise requires, the terms used in this part have the same meaning as set forth in the Fair Credit Reporting Act, 15 U.S.C. §§ 1681 *et seq.*

(b) As used in this part, "Consumer Information" means all records and files of information about an individual, whether in paper, electronic, or other form, that contain a consumer report or information derived from a consumer report.

(c) As used in this part, "derived from" means all information obtained in whole or in part from a consumer report.

(d) As used in this part, "disposing" or "disposal" includes:

(i) the discarding or abandonment of Consumer Information, or

(ii) the sale, donation, transfer, or discarding of any medium, including computer equipment, upon which Consumer Information is stored.

(e) As used in this part, "business purpose" includes the business of government.

§ 682.2 Purpose and scope.

(a) *Purpose.* This part ("rule") implements section 216 of the Fair and Accurate Credit Transactions Act of 2003, which is designed to reduce the risk of consumer fraud and related harms, including identity theft, created by improper disposal of Consumer Information.

(b) *Scope.* This rule applies to any person over which the Federal Trade Commission has jurisdiction, that, for a business purpose, maintains or otherwise possesses Consumer Information or any compilation of Consumer Information.

(i) To the extent that the Gramm-Leach-Bliley Act requires proper disposal of information, the Disposal Rule sets forth the requisite standards under that Act.

§ 682.3 Proper disposal of Consumer Information.

(a) *Standard.* Any person who maintains or otherwise possesses Consumer Information, or any compilation of Consumer Information, for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal. 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.

(b) *General Requirement.* Covered entities 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 the disposal standard stated in Section 682.3(a).

(c) *Outsourcing Requirements.* All covered persons who outsource the destruction of Consumer Information shall conduct due diligence on the record disposal company, enter into a contract governing proper record disposal, and take reasonable steps to monitor contract compliance.

(i) *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, requiring 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.

(d) *Third Party Servicers.*

(i) Third parties, including garbage collectors, recyclers, or records management and storage companies, are not required to make independent determinations about whether the documents in their custody constitute Consumer Information. Such third parties engaged in the normal course of business are exempt from this rule unless and until the following two conditions are met:

(A) The record owner notifies the third party that documents transferred to the third party contain Consumer Information, and

(B) the third party enters a written contract with the record owner to dispose of Consumer Information pursuant to the requirements of this rule.

(ii) Third parties who are not exempt from this rule based on the criteria set forth in Section 682.3(d)(i) shall:

(A) implement and take reasonable steps to monitor compliance with policies and procedures that protect against unauthorized access to or use of Consumer Information during collection and transportation and

(B) dispose of such information in accordance with the standards and requirements of this rule.

§ 682.4 Relation to other laws.

Nothing in this rule shall be construed—

(a) to require a person to maintain or destroy any record pertaining to a consumer that is not imposed under other law; or

(b) to alter or affect any requirement imposed under any other provision of law to maintain or destroy such a record.

§ 682.5 Effective date.

This rule is effective 3 months from the date on which a final rule is published in the Federal Register.