Comment #: 8

Consumers Union
Publisher of Consumer Reports

West Coast Office
1535 Mission St., San Francisco, CA 94103
415-431-6747 (phone) 415-431-0906 (fax)
www.consumersunion.org

May 24, 2004

Office of the Secretary
Federal Trade Commission
by electronic filing

Re: The FACT Act Disposal Rule, R-411007

Consumers Union, the nonprofit publisher *Consumer Reports*, Consumer Federation of America, and U.S. PIRG offer these comments on the FACT Act Disposal Rule as proposed by Federal Trade Commission. This rule is an important part of the identity theft protections offered by the FACT Act. We offer both comments and specific language suggestions to show how these comments could be implemented.

General Comment

We support the result under the rule that a company which contracts with a disposal company to remove and destroy covered documents is responsible not only for reasonable procedures and diligence in selecting the disposal company, but also for the quality of the disposal work. This should prevent the situation where the disposer has satisfied its responsibilities through diligent selection of a disposal company that fails to live up to its promises.

Section 682.1 Definitions

The definition of "consumer information" properly includes information derived from a consumer report. The purpose of the statutory provision would be thwarted if the rule did not extend to information that is derived from a consumer report. For example, a record containing a credit score is derived from, but does not contain, consumer report information. Similarly, allowing affiliates who receive consumer information to dispose of it without being subject to the rule would be a major loophole. We therefore urge that "derived from" be retained in the rule. However, we suggest clarifying that the definition includes information which is derived in whole or in part from a consumer report.

The definition of consumer information should include some records not about specific individuals. A record which contains qualifying information that could be used to impersonate an individual should be included within the definition of consumer information, even if that record does not tie the information to a specific individual. For example, a customer list of Social Security Numbers is the kind of sensitive financial information that ought to be covered by the disposal rule even if that list does not cross-

match customer names to the Social Security Numbers. The numbers alone are ammunition for thieves to use to create new identities.

The definition of consumer information should expressly include compilations. The statute, but not the proposed definition, expressly includes "a compilation." The regulation's definition should be amended to expressly include information that is a compilation containing consumer information.

The definition should be broader with respect to media and equipment. The definition of "disposal" properly includes the sale, donation, or transfer of a medium, including computer equipment, upon which consumer information is stored. However, this subpart of definition 682.1 should be modified to include the discarding of media or equipment, and to expressly include computer media as well as computer equipment. Finally, because the types of media and equipment upon which consumer information may be stored in the future defy present imagination, the rule also should be modified to expressly include, in addition to computer equipment, other non-paper media and equipment for non-paper storage of information.

Section 682.3 Proper Disposal of Consumer Information

The standard is far too general. The explanatory material notes that the disposal rule is modeled on the Safeguards Rule. We are concerned that this makes the rule entirely too general. The rule is unlikely to increase the care with which American businesses handle records containing consumer information if it simply requires reasonable measures without setting any minimum requirement or baseline for what is reasonable. The examples given in subpart (b) would be quite helpful if they were required elements of reasonable measures, rather than merely advisory. If the Commission is not ready to require each of these steps, it should at least recast them as essential conduct to meet the general standard set forth in (a).

Due diligence should ordinarily require more than just references. The problem with a general reasonableness rule is illustrated in section 682.3, which includes a list of things which constitute due diligence, including merely checking several references. Our suggested revisions would tighten this, and would also clarify that there must be conduct satisfying such category in section 682.3(b, thus making that section an argumentation of the general rule in (a), not merely a set of examples.

The rule must address post-disposal access. The disposal rule should require that the measures be taken protect against unauthorized access to use of the information not only in connection with the disposal of the information, but also after the information is disposed of. The rule must protect not only against interception of information during disposal, which could be implied by the phrase, "in connection with its disposal." The rule must also protect against unauthorized access to or use of the information after it has been disposed of. The language could be tightened to clarify this.

The reference to the normal course of business in disposing of garbage in accordance with standard procedures should be clarified. We do not suggest that the rule should impose special conditions on garbage collectors as they dispose of garbage collected in ordinary course of business (as opposed to any disposal they might make of their own customer records containing qualifying consumer information). However, the general reference to "traditional garbage collectors engaging in the normal course of business disposing of garbage in accordance with standard procedures" could be read to suggest that simply putting documents containing sensitive consumer information in the trash for normal garbage pickup is an adequate means of disposal. We understand that this is not the purpose of that language. The language should be tightened to eliminate that implication.

We urge that the disposal rule be strengthened by making these changes. Suggested language that could be used on these points follows. In addition, there is much more to be done, beyond the scope of the disposal rule, to protect consumers from identity theft stemming from the theft of information maintained in business records.

Very truly yours

Gail Hillebrand
Consumers Union of U.S., Inc.

Travis Plunkett
Consumer Federation of America

Ed Mierzwinski
U.S. PIRG

Suggested Language Changes

§ 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 any record about an individual or containing information that could be used to impersonate an individual, whether in paper, electronic, or other form, that is a consumer report or is derived in whole or in part from, or otherwise contains information derived from a consumer report, or is a compilation containing such information.

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

(1) the discarding or abandonment of consumer information, and

(2) the sale, donation, discarding or transfer of any medium, including computer equipment, or computer media, upon which consumer information is stored, or other non-paper media upon which information is stored, or other equipment for non-paper storage of information.

§ 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.

§ 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, or after, its disposal.

(b) ~~Examples.~~ Required areas of activity to meet the standard. Reasonable measures to protect against unauthorized access to or use of consumer information in connection with its disposal ~~would~~ must include, but may not be limited to:

(1) Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers containing consumer information so that the information cannot practicably be read or reconstructed.

(2) Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media and other non-paper media containing consumer information so that the information cannot practicably be read or reconstructed.

(3) 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. In this context, due diligence ~~could~~ should ordinarily include, but may not be limited to, one or more of the following: 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~~,~~ and requiring that the disposal company be certified by a recognized trade association or similar third party with a reputation for high standards of quality review, 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.

(4) (a) For disposal companies explicitly hired to dispose of records containing or derived from consumer information: implementing and monitoring compliance with policies and procedures that protect against unauthorized access to or use of consumer information during or after collection and transportation, and disposing of such information in accordance with examples (1) and (2) above.

(b) For traditional garbage collectors engaged in the normal course of business: ~~disposing of garbage in accordance with standard procedures~~. The normal form of disposing of documents or media by these entities does not satisfy this rule unless the documents or media are first processed as described in (1)-(3). However, this rule does not impose special obligations on traditional garbage collectors engaged in the normal course of business who have not contracted to offer special disposal services for sensitive information.