

Federal Trade Commission Final Rule on Disposal of Consumer Information

On November 18, 2004, the Federal Trade Commission (“FTC”) issued a final consumer information disposal rule. Approximately a year ago, Congress enacted the Fair and Accurate Credit Transactions Act of 2003, Pub. L. No. 108-159, 117 Stat. 1952 (the “FACT Act”). Section 216 of the FACT Act, which is intended to reduce the risk of consumer fraud and identity theft, requires various federal agencies, including 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 of compilation.” *Id.* The recent action by the FTC satisfies this statutory direction.

Last April, the FTC issued, and sought comment on, a proposed disposal rule, and subsequently sought additional comment on the effects of the proposal on small businesses. In total, the FTC received 58 comments, including detailed comments from NAID. Other commenters included the American Insurance Association, America’s Community Bankers, ARMA International, PRISM International, Bank of America Corporation, MasterCard International, Visa U.S.A., the Consumers Union, the Privacy Rights Clearinghouse, the Consumer Federation of California, the Identity Theft Resource Center, Privacy Activism, the Worldwide Privacy Forum, AccuShred, LLC, Allshred Services, Inc., Community Shredders, Indy Shred, Reclamere, Inc., SECURE Eco Shred, and Shred-it Orlando. The final rule considers and responds to many of the comments received.

In addition the FTC rule, the Securities and Exchange Commission and various federal banking agencies (such as the Federal Reserve Board, the FDIC, and the Office of Thrift Supervision) have issued proposed regulations, have received comments on those proposals, and will likely issue final rules over the next several weeks.

We set forth below some of the highlights of the FTC final rule on the disposal of consumer report information and records:

Effective Date

The FTC rule will take effect on June 1, 2005. Those subject to the rule will, accordingly, have the next six months to bring their operations into compliance.

Covered Persons

The rule states that it “applies to any person over which the Federal Trade Commission has jurisdiction, that, for a business purpose, maintains or otherwise possesses consumer information.” The FTC has jurisdiction over the vast majority of US businesses, but its jurisdiction does not extend to a few sectors, including banking and insurance. In commentary

accompanying the final rule, the FTC has indicated that it will construe the phrase “for a business purpose” broadly to cover all business reasons a company may possess consumer information. In short, anyone who possesses consumer information, with the exception of an individual consumer who has obtained his or her own consumer report, may be subject to the disposal rule. Covered entities include:

- Consumer reporting agencies;
- Lenders;
- Employers;
- Landlords;
- Government agencies;
- Mortgage brokers;
- Automobile dealers;
- Other users of consumer reports; and
- Service providers, like disposal and record storage companies that receive, hold and dispose of consumer reports on behalf of their customers.

Covered Information

The rule broadly covers “any record about an individual, whether in paper, electronic, or other form, that is a consumer report”—also known as a credit report—“or is derived from a consumer report.” Consumer information also includes compilations of such records. However, consumer information excludes aggregate data and other information that does not identify individuals by listing their names or other information that could be used for identification purposes, such as social security numbers. The rule applies to all media, so it does not matter whether the consumer information appears on the printed page, on a computer hard drive, on a CD, DVD, disk, or in any other form. The process for properly disposing of consumer information, however, may—of course—differ depending on the media at issue.

Covered Conduct

The rule does not regulate how companies protect sensitive information they maintain in their files (though that information may be protected under other laws), but rather applies to the “disposal” of consumer information. “Disposal” is defined to mean the discarding or abandonment of consumer information and “the sale, donation, or transfer of any medium, including computer equipment, upon which consumer information is stored.” The commentary

accompanying the final rule makes clear, however, that the disposal rule (as opposed to other rules) does not apply to the mere sale, donation, or transfer of the consumer information itself.

Ensuring Proper Disposal

The rule does not provide specific directions regarding the proper disposal of consumer information, but rather requires covered persons to “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.” Under this standard, a covered person is not required “to ensure perfect destruction of consumer information in every instance,” but rather “to take reasonable measures to protect against unauthorized access or use of the information in connection with its disposal.” As explained in its commentary, the FTC will consider a number of factors—including “the sensitivity of the consumer information, the nature and size of the entity’s operation, the costs and benefits of different disposal methods, and relevant technological changes—in assessing the “reasonableness” of the measures taken.

Although not required as a matter of law, the rule does provide a number of examples to offer guidance on disposal measures that would satisfy the “reasonableness requirement.” These examples, which are “illustrative only and . . . not exclusive or exhaustive,” include:

- “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.
- “Implementing and monitoring compliance with policies and procedures that require the destruction or erasure of electronic media containing consumer information so that the information cannot practicably be read or reconstructed.”
- “For person subject to the Gramm-Leach-Bliley Act, 15 U.S.C. 6081 *et seq.*, and the [FTC’s] Standards for Safeguarding Consumer Information, 16 C.F.R. Part 314 (“Safeguard Rule”)”—that is, financial institutions such as lenders and debt collectors —“incorporating the proper disposal of consumer information as required by this rule into the information security program required by the Safeguards Rule.”

Two of the examples given by the FTC are of particular interest to those in the records disposal and records storage businesses.

First, the examples provide that a covered person can satisfy his or her obligations under the rule by, “[a]fter due diligence, entering into and monitoring compliance with a contract with another person engaged in the business of record destruction to dispose of material, specifically identified as consumer information, in a manner consistent with this rule.” In short, a consumer reporting agency, a lender, an insurer, an employer or any other covered entity, can satisfy the rule by contracting with a qualified record disposal company to destroy the records at issue and monitoring compliance with that contract. The rule, in turn, describes due diligence to 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.

These examples are important because they outline the ways in which service providers—that is, shredding and other information disposal companies—will likely be assessed by their customers and potential customers.

Second, the rule makes clear that it applies, not only to many customers of shredding and other information disposal companies, but also to “service providers”—including information storage and disposal companies themselves. One of the examples of “reasonableness” provides some guidance regarding how the rule might apply to service providers. The example provides:

For persons or entities who maintain or otherwise possess consumer information through their provision of services directly to a person subject to this part, implementing and monitoring compliance with policies and procedures that protect against unauthorized or unintentional disposal of consumer information, and disposing of such information in accordance with [the examples discussed in the first two bullet points above].

Based on this example, it will be important for service providers to adopt appropriate disposal policies and procedures and to implement a compliance monitoring system if they have not already done so.

The commentary to the rule explains that a service provider’s compliance will be evaluated based on whether a record owner provided notice that consumer information was included or contracted for disposal, in addition to the following factors:

- Actual or constructive knowledge of the nature of the consumer information;
- The course of dealing between the service provider and record owner;
- The sensitivity of the consumer information;

- The nature and size of the service provider’s operations; and
- The costs and benefits of different disposal methods.

The commentary further stresses that “[i]n evaluating a service provider’s compliance with this Rule . . . a record owner’s failure to provide notice or contract for disposal in accordance with the requirements of the Rule will be strongly considered.” In light of these requirements, individual service providers may want to consult with their counsel regarding how best to ensure their compliance and whether any modification to their customer contracts is appropriate.

Penalties

Penalties for violating the rule include actual damages, statutory damages up to \$1,000 per customer (with no cap on class action damages) for willful violations, punitive damages, attorneys’ fees, and civil penalties up to \$2,500.