

If You Don't Think the FACTA Disposal Rule Applies To You, Think Again!

Charles H. Kennedy
Counsel, Morrison & Foerster, LLP

INTRODUCTION

On its face, the Disposal Rule adopted by the Federal Trade Commission (“FTC” or “Commission”) to enforce the records disposal requirements of the Fair and Accurate Credit Transactions Act (“FACTA”) appears to apply only to limited sets of circumstances. Specifically, the Rule purports to apply only to the proper disposal of information derived from consumer credit reports; covers only information retained for a business purpose; and appears to apply only to consumer information, rather than information that pertains to businesses or their employees.

In fact, these apparent limitations will have little effect on enforcement of the Disposal Rule. As the FTC has demonstrated in its handling of other privacy-related statutes, the Commission will stretch the Disposal Rule’s reach until it effectively covers nearly all entities that retain and dispose of personal information for any purpose.

Specifically, we must expect the Commission to apply this Rule to all personal information, including employee information and information not expressly based on consumer credit reports that is maintained by any organization. We also can expect the Disposal Rule’s standards to be used by private plaintiffs as an indirect basis for lawsuits against governmental organizations that mishandle personal information.

Charles H. Kennedy has taught cyberlaw and communications law for the past ten years at the Columbus School of Law, Catholic University of America, and is an author of four books on the law of electronic communications. He is Of Counsel to Morrison & Foerster, LLP, where he can be reached at ckennedy@mofo.com.

I. WHAT THE DISPOSAL RULE SAYS

In 2003, Congress adopted the Fair and Accurate Credit Transactions Act,¹ which extensively amended the existing Fair Credit Reporting Act (“FCRA”).² FACTA’s provisions were intended primarily to help consumers prevent, or at least reduce the harm from, identity theft. But, the new statute also required that “any person that maintains or otherwise possesses consumer information, or any compilation of consumer information, derived from consumer reports for a business purpose [must] properly dispose of such information or compilation.”³ The statute directed the federal banking regulatory agencies -- the National Credit Union Administration, the Securities and Exchange Commission, and the Federal Trade Commission – to adopt regulations for the enforcement of this disposal requirement. Such regulations have since been adopted by all of the responsible agencies.⁴

The most extensive such regulations are found in the “Disposal Rule” adopted by the FTC on November 24, 2004, and effective June 1, 2005. According to the Disposal Rule, any person who maintains or otherwise possesses 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.”⁵ Reasonable measures include, but are not limited to, the following examples:

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 containing consumer information so that the information cannot practicably be read or reconstructed.
3. 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.
4. 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 examples (1) and (2) above.
5. For persons subject to the Gramm-Leach-Bliley Act, 15 U.S.C. 6081 et seq., and the Federal Trade Commission’s Standards for Safeguarding Customer Information, 16 CFR Part 314 (“Safeguards Rule”), incorporating the proper disposal of consumer information as required by this rule into the information security program required by the Safeguards Rule.⁶

The Disposal Rule also includes some important definitions. Notably, “dispose,” “disposing” or “disposal” are defined to include both the discarding and abandonment of consumer information and the “sale, donation, or transfer of any medium, including computer equipment, upon which consumer information is stored.”⁷ Also, “consumer information” is defined to include “any record about an individual, whether in paper, electronic, or other form that is a consumer report or is derived from a consumer report.”⁸

A “consumer report,” in turn, has the same definition given to that term in the Fair Credit Reporting Act: “any written, oral, or other communication of any information by a consumer reporting agency bearing on a consumer’s credit worthiness, credit standing, credit capacity, character, general reputation, personal characteristics, or mode of living which is used or expected to be used or collected in whole or in part for the purpose of serving as a factor in establishing the consumer’s eligibility for [credit, insurance, employment or certain other permitted purposes].”⁹

Violations of the Disposal Rule can result in FTC enforcement actions, with the prospect of onerous consent decrees and civil penalties of up to \$2,500 per violation. In the case of a large-scale compromise of information, the FTC might choose to treat the release of each affected individual’s consumer information as a separate violation, raising the possibility of a huge penalty assessment resulting from a single, careless act of disposal.

II. THE DISPOSAL RULE’S BROAD SCOPE

If the FTC’s past enforcement practices are any guide to the future, the Commission already is looking for enterprises that have violated the Disposal Rule. The Commission may find its targets by taking tips from disgruntled employees, or from reports of losses of consumer data caused by failure to dispose properly of that data or the physical media on which it is maintained. The likelihood of such discoveries is enhanced by the dozens of state laws that require organizations to notify consumers of any incident that might have compromised their information.¹⁰

When it finds those unfortunate targets, the Commission will pursue them with costly investigations and will, where warranted, impose lengthy consent decrees, fines and penalties. State authorities very likely will bring their own “me too” actions against those same enterprises, and the plaintiffs’ class action bar will not be far behind.

As frightening as this prospect should be, some organizations will be lulled by the plain words of the statute into a false – and potentially costly – complacency. After all, the Disposal Rule only applies to consumer data, and some companies do not deal directly with consumers at all. Also, even where a company maintains consumer data, the Rule appears not to apply unless consumer data is derived from consumer credit reports. Finally, some types of organizations are not even within the jurisdiction of the FTC.

The following considers each of these comforting rationalizations in turn, and shows just how dangerously naïve they are.

A. “My Company Doesn’t Handle Consumer Information”

Organizations that do not sell directly to consumers, or do not maintain lists of individual purchasers and potential purchasers of their goods and services, may conclude that they have no information subject to the Disposal Rule. The Commission has made it clear, however, that “consumer information” for purposes of the Disposal Rule includes “any record about an individual...”¹¹ An individual, in turn, may not only be a customer or potential customer of the entity, but may be any employee or other person about whom records are maintained. As the Commission’s Order adopting the Disposal Rule points out, “among the entities that possess or maintain consumer information for a business purpose are consumer reporting agencies, as well as lenders, insurers, employers, landlords, government agencies, mortgage brokers, automobile dealers, and other users of consumer reports.”¹²

In the Commission’s view, therefore, any enterprise that conducts background investigations of employees or otherwise stores and disposes of personnel records is subject to the Disposal Rule. And, as we discuss further below, the FTC will interpret the Rule as reaching all personal information concerning employees and other individuals, whether or not that information is directly or indirectly derived from a consumer report. Accordingly, any enterprise with employees should consider itself subject to the Disposal Rule, even if it maintains no information at all concerning consumers not employed by the enterprise.

B. “My Company Doesn’t Handle Information Derived from Consumer Reports”

As noted earlier, FACTA was enacted as a set of amendments to the Fair Credit Reporting Act, a law that regulates credit reporting agencies and users of consumer credit reports. For that reason, FACTA’s disposal requirements, and the implementing rules adopted by the FTC and other responsible agencies, apply specifically to the proper disposal of any information “that is a consumer report or is derived from a consumer report.”¹³ As with other provisions of the Disposal Rule, however, this apparent restriction should not be taken as a serious limitation on the Rule’s scope. In fact, there are at least two reasons to expect that the limitation will be meaningless in practice.

First, organizations are likely to maintain considerable information that originated in credit reports but that no longer is clearly labeled as such. Notably, customer files and personnel records may contain credit report-based data that were acquired as part of a decision to extend credit, screen potential employees or for other purposes. The FTC will require organizations to dispose of such information in accordance with the Disposal Rule, *even if the organization and its responsible records managers do not know that the information is derived from a credit report.*¹⁴ Accordingly, the prudent course is to treat all information about individuals as subject to the Rule.

Second, and more fundamentally, the FTC has stated that “although the Disposal Rule applies to consumer reports and the information derived from consumer reports, the FTC encourages those who dispose of any records concerning a consumer’s personal or financial information to take similar protective measures.”¹⁵ As experienced FTC watchers know, a comment of this kind is much more than a word of “encouragement.” With this benign-sounding bit of language, the Commission is announcing its intention to enforce the Disposal Rule against all organizations that maintain personal information, even where that information is not a consumer report or derived from a consumer report.

To understand how the Commission can expand the FACTA disposal requirements beyond their intended scope, it is necessary to know that the FTC also has another, powerful law at its disposal – specifically, Section 5 of the Federal Trade Commission Act.¹⁶

In Section 5, Congress gave the FTC broad power to regulate all “unfair or deceptive acts or practices” involving interstate or foreign commerce.¹⁷ The Commission has made vigorous use of this authority to prevent and punish false advertising, fraudulent schemes and consumer scams of all kinds.

The Commission’s first involvement in data security and protection was its enactment of regulations (known as the “Safeguards Rule”) to implement the data security requirements of the Gramm-Leach-Bliley Financial Modernization Act (“GLBA”).¹⁸ Like the Disposal Rule, the Safeguards Rule was supposed to have only limited application. Specifically, the GLBA authorized the Commission to adopt regulations that applied only to financial institutions not within the jurisdiction of other agencies. Nothing in the GLBA authorized the Commission to apply the Safeguards Rule to non-financial industries or lines of business.

Despite this clear statutory limitation, the FTC used its Section 5 authority to turn the Safeguards Rule into a de facto information security standard for all U.S. businesses. The Commission began its campaign by attacking companies that failed to implement promised data security measures.¹⁹ (Such failures to live up to published data security commitments were characterized by the FTC as “deceptive” under Section 5.) More recently, the FTC has attacked substandard data security practices as “unfair” under Section 5, even where the target company had made no claims whatever about data security.²⁰

In each of these data security enforcement actions, the FTC required the target company to enter into a 20-year consent decree that committed the company to implement the full complement of security measures required by the Safeguards Rule – including technical, administrative and physical safeguards that may have had nothing to do with the deficiencies that had led to the Commission’s original complaint. Specifically, the consent decrees all required the target companies to establish, implement and maintain comprehensive security programs that were reasonably designed to protect the security, confidentiality and integrity of personal information. Those programs were required to include the following elements:

- Designation of an employee or employees to coordinate and be accountable for the information security program;
- Identification of material internal and external risks to the security, confidentiality and integrity of personal information that could result in the unauthorized disclosure or other compromise of the information, and assessment of the sufficiency of any safeguards in place to control the risks; and
- Design and implementation of reasonable safeguards to control the risks identified through risk assessment, and regular testing or monitoring of the effectiveness of the safeguards’ key controls, systems and procedures.

The message to American business was clear: the Safeguards Rule applies to everyone.

There is no doubt that the Commission will take the same approach to enforcement of the Disposal Rule that it took with the Safeguards Rule. In fact, the Commission already has strongly implied, in the Disposal Rule and other public statements, that failure to comply with the Disposal Rule *will be considered a violation of the Safeguards Rule.*²¹ The Commission’s intention could hardly be clearer: the Disposal Rule, like the Safeguards Rule, applies to disposal of all personal information, whether or not derived from a consumer report, by any entity within the FTC’s jurisdiction.

C. “My Company Is Not Regulated By The FTC”

The FTC has the broadest jurisdiction of any consumer protection agency. The exceptions to its jurisdiction, as enumerated in the FTC Act, are narrow and include regulated common carriers and certain categories of financial institutions.²² Unless your company is clearly within one of the enumerated categories, you should anticipate that the FTC will assert its jurisdiction over you under Section 5 of the FTC Act, including enforcement of the Disposal Rule.

Even if your organization falls outside the FTC’s jurisdiction, you most probably are subject to regulations of another agency, such as the Federal Reserve Board, the Securities and Exchange Commission or a state consumer protection agency, that imposes essentially identical FACTA disposal obligations. That agency, like the FTC, will be empowered to act against violators of its disposal rules.²³

Finally, even in the unlikely event that your organization is not subject to any federal agency’s equivalent of the Disposal Rule, failure to observe the Rule’s requirements may result in adverse legal action. Notably, state consumer protection authorities regulate unfair and deceptive practices under the states’ own statutes, which may grant state authorities jurisdiction over entities not regulated by the FTC or other federal agencies. The states have been aggressive enforcers of privacy and data security, and can be expected to look to federal statutes and regulations, including the Disposal Rule, for guidance as to the level of care they should require of companies that handle and dispose of personal data.²⁴ Similarly, private plaintiffs, including the aggressive class action bar, will rely upon state consumer protection laws as the basis for suits that seek large damage awards and payment of attorneys’ fees by unsuccessful defendants.²⁵ Evidence in support of such private actions may include the defendants’ failure to comply with accepted disposal practices, as represented most authoritatively by the Disposal Rule.

D. “My Organization Is A Government Agency”

Agencies of federal, state and local governments may assume that their records disposal practices are immune from scrutiny under FACTA and the Disposal Rule, but the Congress and the FTC have declared otherwise. Notably, the Fair Credit Reporting Act, into which the FACTA requirements are incorporated, defines the class of persons to which FCRA applies to include “any individual partnership, corporation, trust, estate, cooperative, association, government or governmental subdivision or agency, or other entity.”²⁶ Consistent with this statutory language, the FTC lists “government agencies” among the entities that must comply with the Disposal Rule.²⁷

As an obligation of federal agencies, in particular, the Disposal Rule can be read as supplementing and clarifying the existing duties of such agencies under the Privacy Act of 1974.²⁸ Specifically, the Privacy Act requires federal agencies to “establish appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained.”²⁹ If an agency “fails to comply with [these provisions] in such a way as to have an adverse effect on an individual,” that aggrieved individual may bring a civil action against the offending agency in which an award of damages, costs and attorneys’ fees to the plaintiff may be made.³⁰

In future civil actions brought under the data security and integrity provisions of the Privacy Act of 1974, courts are likely to look to the Disposal Rule as a source of the standard to which defendant agencies must be held in their disposal of records concerning individuals.

State and local government agencies also are subject to the FCRA, FACTA and the Disposal Rule, and multiple means of enforcing those agencies’ obligations are available. Besides direct enforcement action under the Disposal Rule, many states have laws that are counterparts to the federal Privacy Act of 1974. Also, aggravated violations of the rights of citizens to secure and accurate information can result in civil claims, including suits for violations of the affected individuals’ civil rights.³¹

III. CONCLUDING THOUGHTS

All U.S. enterprises that maintain personal information should be aware that the FTC is likely to make the Disposal Rule an enforcement priority in the very near future. Such an initiative would follow a familiar pattern, in which the FTC adopts a new rule or otherwise announces an interest in a privacy-related subject, then moves aggressively to bring enforcement actions entities that fail to address the FTC’s concerns in ways the Commission thinks appropriate.

For example, the Commission held hearings, beginning in the mid-1990s, concerning online collection of personal information and issued reports on that subject in 1998, 1999 and 2000.³² The Commission at first supported industry self-regulation as the preferred method of protecting online privacy, but in its 2000 Report urged the Congress to pass comprehensive online privacy legislation. Even in the absence of such legislation, the FTC used its Section 5 authority against companies that failed to protect the privacy of information submitted online.³³

Similarly, after it introduced its GLBA Safeguards Rule and while final adoption of that Rule was pending, the Commission opened a data security initiative, including its “Dewie the Turtle” public education campaign on the subject of online security and information protection.³⁴ That same year saw the FTC’s enforcement action against Eli Lilly, which proved to be the first of a series of actions against companies that allegedly had failed to protect personal information stored on their networks.

With the adoption of the Disposal Rule, the FTC has a new enforcement tool aimed specifically at the problem of careless disposal of personal information and the physical media on which that information is stored. The Commission will move promptly to demonstrate its commitment to the disposal issue, and organizations that falsely believe themselves to be exempt from the Disposal Rule may be among the first targets.

Footnotes

- ¹ Fair and Accurate Credit Transactions Act of 2003, Pub.L. 108-159, 111 Stat. 1952 (“FACTA”).
- ² Fair Credit Reporting Act, 15 U.S.C. § 1681 et seq.
- ³ FACTA § 216, 15 U.S.C. § 1681w(a)(1).
- ⁴ See Office of the Comptroller of the Currency, Federal Reserve System, Federal Deposit Insurance Corporation, Office of Thrift Supervision, *Amendments to Interagency Guidelines Establishing Standards for Safeguarding Customer Information* (effective July 1, 2005).
- ⁵ 16 C.F.R. Pt. 682 § 682.3(a).
- ⁶ *Id.* § 682.3(b).
- ⁷ *Id.* § 682.1(c).
- ⁸ *Id.* § 682.1(b). Consumer information “does not include information that does not identify individuals, such as aggregate information or blind data.” *Id.*
- ⁹ Fair Credit Reporting Act, 15 U.S.C. § 1681.a(d)(1). A consumer reporting agency is defined as “any person which, for monetary fees, dues, or on a cooperative nonprofit basis, regularly engages in whole or in part in the practice of assembling or evaluating consumer credit information or other information on consumers for the purpose of preparing consumer reports to third parties, and which uses any means or facility of interstate commerce for the purpose of preparing or furnishing consumer reports.” *Id.* § 1681.a(f).
- ¹⁰ Cal. Civ. Code § 1798.82 (West 2003); Ark. SB 1167 (2005); Conn. SB 650 (2005); Del. HB 116 (2005); Fla. HB 481 (2005); Ga. SB 230 (2005); Ill. HB 1663, Public Act 094-0036 (2005); Ind. Act No. 503 (2005); La. SB 205, Act 499 (2005); Me LD 1671 (2005); Minn. H.F. 2121 (2005); Mont. HB 732(2005) NJ A 4001/S1914 (2005); NY A4252, A3492 (2005); Nev. SB 347 (2005); NC SB 1048 (2005); ND SB 2251 (2005); RI H. 6191 (2005); Tenn. SB 2220 (2005); Tex. SB 122 (2005); Wash. SB 6043 (2005).
- ¹¹ 16 C.F.R. Pt. 682 § 682.1(b).
- ¹² Federal Trade Commission, *Final Rule, Disposal of Consumer Information and Records*, 69 Fed. Reg. 68690, 68693 (Nov. 24, 2004) (*emphasis added*).
- ¹³ 16 C.F.R. Pt. 682 § 682.1(b).
- ¹⁴ 69 Fed. Reg. 68690, 68692. “[T]he Commission notes that knowledge is not an element or a prerequisite to the duty to comply with either the FACTA Act or the Disposal Rule.” *Id.*
- ¹⁵ Federal Trade Commission, “FACTA Disposal Rule Goes Into Effect June 1,” <http://ftc.gov/opa/2005/ob/disposal.htm>.
- ¹⁶ 45 U.S.C. § 45(a).
- ¹⁷ *Id.*
- ¹⁸ Pub.L. 106-102, 113 Stat. 1338 (1999). The Safeguards Rule can be found at 16 C.F.R. Pt. 314.
- ¹⁹ See, e.g., *Eli Lilly and Co.*, Docket No. C-4047 (May 8, 2002), <http://www.ftc.gov/opa/2002/01/elililly.htm>; *In the Matter of Microsoft Corp.*, File No. 012-3240, <http://www.ftc.gov/opa/2002/08/microsoft.htm>; *In the Matter of GUESS?, Inc., a corporation, and GUESS.COM, Inc., a corporation*, File No. 022-3260, <http://www.ftc.gov/os/2003/06/guesscmp.htm>; *In the Matter of MTS, Inc., doing business as Tower Records/Books/Video, a corporation and Tower Direct, LLC doing business as Tower Records.com, a corporation*, File No. 032-3209, <http://www.ftc.gov/os/caselist/0323209.htm>.
- ²⁰ *In the Matter of BJ’s Wholesale Club*, Docket No. C-4148, Decision and Order (Sep. 23, 2005).
- ²¹ 16 C.F.R. Pt. 682 § 682.3(b)(5); 69 Fed. Reg. 68690, 68693 (“[C]ompliance with the standards of the Disposal Rule will constitute compliance with the disposal obligations under the Safeguards Rule.” *Id.*).
- ²² “The Commission is hereby empowered and directed to prevent persons, partnerships, or corporations, except banks, savings and loan institutions described in section 57a(f)(4) of this title, common carriers subject to the Acts to regulate commerce, air carriers and foreign air carriers subject to part A of subtitle VII of Title 49, and persons, partnerships, or corporations insofar as they are subject to the Packers and Stockyards Act, 1921, as amended..., from using unfair methods of competition in or affecting commerce and unfair or deceptive acts or practices in or affecting commerce.” 15 U.S.C. § 45(a)(2).
- ²³ See, e.g., *Interagency Guidelines* cited at footnote 5, *supra*.

- ²⁴ See, e.g., *In the Matter of Ziff Davis Media Inc., Assurance of Discontinuance effective Aug. 28, 2002*, Office of New York State Attorney General, www.oag.ny.us; *State of Ohio v. DSW, Inc.*, Case No. 05CV06-6128 (Complaint for Declaratory Judgment, Court of Common Pleas, Franklin County, Ohio, June 6, 2005), Press Release of Attorney General Jim Petro at http://www.ag.state.oh.us/press_releases/2005/pr20050606.htm.
- ²⁵ See, e.g., *Parke et al. v. Cardsystems Solutions, Inc., et al.*, Case No. CGC-05-442624 (Cal. Sup. Ct., First Amended Complaint filed July 5, 2005); see also *Helen Remsburg, Administratrix of the Estate of Amy Lynn Boyer v. Docusearch, Inc.*, 149 N.H. 148, 816 A.2d 1001 (Sup. Ct. N.H. 2003).
- ²⁶ 15 U.S.C. § 1681.a(b)(emphasis added).
- ²⁷ Federal Trade Commission, "FACTA disposal Rule Goes Into Effect June 1" (Press Release of June 1, 2005), <http://www.ftc.gov/opa/2005/06/disposal.htm>.
- ²⁸ 5 U.S.C. § 552 ("Privacy Act").
- ²⁹ *Id.* § 552e(10).
- ³⁰ *Id.* § 552g.
- ³¹ See, e.g., *Rogan v. City of Los Angeles*, 668 F.Supp. 1384 (C.D. Cal. 1987).
- ³² See Federal Trade Commission, "Privacy Online: A Report to Congress" (June 1998); "Self-Regulation and Privacy Online" (July 1999); "Privacy Online: Fair Information Practices in the Electronic Marketplace, A Report to Congress" (May 2000); available at <http://ftc.gov>.
- ³³ See *FTC v. ReverseAuction.com, Inc.*, No. 00-0032 (D.D.C. Jan. 6, 2000); *Liberty Financial Companies, Inc.*, FTC Docket No. C-3891 (Aug. 12, 1999); *GeoCities*, FTC Docket No. C-3849 (Feb. 12, 1999).
- ³⁴ See FTC News Release, "FTC Introduces Internet Safety Mascot, 'Dewie the Turtle,' at Privacy 2002 Conference" (Sep. 26, 2002), <http://ftc.gov/opa/2002/09/dewie.htm>.

© 2005 Iron Mountain Incorporated. All rights reserved. Iron Mountain and the design of the mountain are registered trademarks of Iron Mountain Incorporated. All other trademarks are the property of their respective owners.



745 Atlantic Avenue
Boston, Massachusetts 02111
(800) 899-IRON

Iron Mountain operates in major markets worldwide, serving thousands of customers throughout the U.S., Europe, Canada, Latin America, and the Pacific Rim. For more information, visit our Web site at www.ironmountain.com.