

[Download this article in PDF format.](#)

How Well Are You Safeguarding Your Employees' Personal Data?

New Federal Rule on Disposal Took Effect June 1, 2005

By **Christine Martin**

In February, Choice Point, an Atlanta-based data broker, disclosed that identity thieves had stolen personal information on 145,000 consumers nationwide. In September, the University of Georgia reported that an overseas hacker had accessed the social security numbers of approximately 1600 employees working for its College of Agricultural and Environmental Sciences.

Now a new federal rule requires businesses that compile or maintain personal data based on consumer reports, including that compiled on employees, to completely destroy such information before they discard it. The new rule on the "Disposal of Consumer Report Information and Records" promulgated by the Federal Trade Commission under the 2003 Fair and Accurate Credit Transactions Act (FACTA), took effect June 1, 2005.¹ It requires businesses such as landlords, lenders, debt collectors, insurance companies, and consumer reporting companies to take "reasonable measures to protect against unauthorized access to or use of" any personally identifiable information regarding employees when the records are discarded. At least one law firm, Baker and Daniels, which has offices in Indianapolis and Washington, D.C., has opined that the new rule applies to "all employers."² An FTC "business alert" posted on its web site ([Disposing of Consumer Report Information? New Rule Tells How](#)) also lists employers among those covered by the rule.³

According to the rule, "reasonable measures" that an employer may take to ensure that personal information, such as social security numbers, does not fall into the wrong hands include the "burning, pulverizing, or shredding of papers" and the "destruction or erasure of electronic media" so that "the information cannot practicably be read or reconstructed."

Even though the new rule applies to only information derived from consumer reports, the FTC on its web site "encourages those who dispose of any records containing a consumer's personal or financial information to take similar protective measures." The definition of consumer report is broader than one might think. According to the FTC, it is "information that is used—or expected to be used—in establishing a consumer's eligibility for credit, employment, or insurance, among other purposes." According to the FTC, "credit reports and credit scores are consumer reports." So are reports that relate to employment background, check writing history, insurance claims, residential or tenant history, or medical history."⁴

According to Baker and Daniels, victims are entitled to recover actual damages "sustained as a result of a violation of the rule" and may seek statutory damages of up to \$1000 per violation. Willful violation by an employer may invite punitive damages or a class action lawsuit.

Certainly a good records management or information security program can pay off in improved employee relations as well as reduced exposure to legal liability. The range of personal information on employees that appears in company files is truly daunting. For example, depending on an organization's security and pre-employment screening practices, information held by an employer on an employee could include:

- fingerprint or other biometric identifier
- medical records
- driver's license number
- photograph

- university transcripts
- disciplinary files
- bank account numbers, especially if the employer offers direct deposit of paychecks
- birth date
- vehicle license plate or vehicle identification number (VIN), especially if the employer issues parking permits
- personal investment decisions directing assets in pension plans or life insurance policies, including names and social security numbers of beneficiaries
- drug test results
- polygraph test results
- psychological or personality test results
- payroll deduction information, including
 - charities or advocacy groups a worker chooses to support;
 - any payroll deductions an employee may have authorized to pay for automobiles or other big-ticket items; and
 - any court-ordered payments for child support or other debts, including those that may result in an employee's wages being garnished.

Libraries, perhaps more than most employers, already recognize the importance of safeguarding personal information. After all, the American Library Association has had a policy on safeguarding library users' personal information since 1991.⁵ Certainly, libraries will appreciate that employees may not want others to know that their wages are being garnished or that their payroll deductions support an unpopular political cause.

The following organizations represent individuals employed in records management and human resources (HR) information technology. Contact them to learn more about records management and information security programs to safeguard employee information and all of an organization's information assets.

- ARMA International (originally founded as the Association of Records Managers and Administrators) (www.arma.org)
- International Association for Human Resources Information Management (www.ihrim.org).

In general, a good records management program consists of:

- A records inventory that identifies the organization's record series (e.g., time sheets, group insurance contracts, employment applications, and other records generated by the employer on a regular basis). Ideally, the inventory will indicate:
 - who has access to the record;
 - what protected personal information it contains;
 - what laws require the organization to make it public or keep it private;
 - who has custody of the official copy;
 - who has other, or convenience, copies; and
 - how long it must be kept (i.e., a records retention schedule).
- Perhaps most crucial: Support from senior management, who will direct the following departments to participate: records management, legal, information technology, finance, human resources, and risk management.
- Timely destruction of records to prevent unauthorized access and to free up space.
- Periodic audits to determine how well employees are following records management policies.
- An awareness of how to dispose of electronic records (i.e., electronic records are not necessarily destroyed just because someone has deleted them—they may continue to exist on backup tapes, in folders full of “deleted items,” and as attachments to other people's email).
- A way to prevent the otherwise-scheduled destruction of records needed for pending audits or litigation.
- An effort to educate employees about records retention policies. Presenting records management as a way to prevent identity theft may help sell a program that might otherwise seem to lack any direct benefit to most employees.

References

1. 16 Code of Federal Regulations 682 Disposal of Consumer Report Information and Records. Published in the Federal Register, page 68690, on November 24, 2004.
2. Baker and Daniels, LLP, Indianapolis, Indiana, and Washington, D.C., “Special Employment Alert: New Rule on Disposal of Employee Identity Information Effective June 1, 2005,” June 2005. (www.inla1.org/specialemploymen.htm)
3. Federal Trade Commission. FTC Business Alert: Disposing of Consumer Report Information? New Rule Tells How, June 2005. (www.ftc.gov/bcp/online/pubs/alerts/disposalalrt.htm)

4. Federal Trade Commission. FTC Business Alert: Disposing of Consumer Report Information? New Rule Tells How, June 2005. (www.ftc.gov/bcp/online/pubs/alerts/disposalalrt.htm)
 5. "Policy Concerning Confidentiality of Personally Identifiable Information about Library Users," adopted July 2, 1991, by the American Library Association Council. (www.ala.org).
-

Christine Martin is a freelance writer and 1997 graduate of the [University of Illinois Graduate School of Library and Information Science](#).

We would love to have your [feedback](#) on this article!

Copyright 2004–2005 ALA-APA. Contact Jenifer Grady, 50 E. Huron, Chicago, IL 60611, 312-280-2424, jgrady@ala.org for more information.