

## Cleaning House: The New Federal “Disposal Rule” Provides Guidelines for Disposing of Certain Personnel Records

By Nichole Chiappini

Concerned over the growing problem of identity theft, in December 2003, Congress passed the Fair and Accurate Credit Transactions Act (the FACT Act). Among other things, the FACT Act directed the Federal Trade Commission (FTC) to issue regulations that require businesses to “properly dispose” of consumer information. The FTC issued its regulations in November 2004. The regulations, collectively referred to as “the Disposal Rule,” became effective June 1, 2005. This Note discusses the Disposal Rule, how it applies to employers, and the penalties for violating the Rule.

**THE DISPOSAL RULE.** Under 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 information” both during and after its disposal.

**What is “Consumer Information?”** Several layers of definitions are needed to understand what information is subject to the Disposal Rule. First, “consumer information” is any record, or compilation of records, about an individual that is contained in or derived from a *consumer report*. Second, in the context of employment, a “consumer report” is any information provided by a *consumer reporting agency* that relates to an individual’s credit worthiness, character, general reputation, or personal characteristics that is used for determining employment eligibility. Third, a “consumer reporting agency” is any person or entity that regularly assembles or evaluates information about consumers for the purpose of providing it to third parties.

Therefore, the Disposal Rule only applies to identifying information that is contained in or derived from a consumer report that was provided by a consumer reporting agency. The Rule applies to such information regardless of whether it is in paper or electronic form. The Rule does not apply to information that does not identify individuals, such as aggregate information of blind data, even if the information was provided by a consumer agency.

**What are “Reasonable Measures?”** The Disposal Rule does not require businesses to ensure perfect destruction of consumer information. Instead, it requires that businesses take “reasonable measures” to protect against unauthorized access to or use of the information in connection with its disposal. The “reasonable measures” standard is not intended to be vague; rather, it is intended to be flexible, taking into account the unique circumstances of a particular business. Accordingly, when determining whether a business has taken reasonable measures to dispose of consumer information, the FTC will consider multiple factors. These factors include, but are not limited to: (1) the sensitivity of the consumer information; (2) the nature and size of the business (3) the costs and benefits of different disposal methods; (4) relevant technological changes; (5) whether business establishes policies and procedures governing disposal; and (6) whether the business trained its employees regarding such establishment policies and procedures. No single factor is determinative.

**HOW THE RULE APPLIES TO EMPLOYERS.** As part of the hiring process or workplace investigations, many employers perform background checks on prospective and current employees. If, during the course of such a background check, an employer uses a third party to obtain information on the prospective or current employee (*e.g., credit bureau or private investigator*), then that information is subject to the Disposal Rule. The Report and any information derived from it, whether in paper or electronic form, must be disposed of properly.

**Does the Rule Require Disposal of Personnel Records?** The Disposal Rule does not require employers to dispose of personnel records that contain consumer information. The Rule merely sets forth the standard that employers must meet if they choose to, or are required by another law to, dispose of such records.

However, before disposing of any personnel record — regardless of whether they contain consumer information — employers need to keep in mind that various other laws require them to retain certain records for specific periods. For example, regulations related to the Age Discrimination in Employment Act (ADEA) require retention of job applications and résumés for one year, and regulations related to the Immigration Reform and Control Act (IRCA) require employers to retain records related to employment eligibility for three years after the date of hire or for one year after the date of termination, whichever is later.

**PENALTIES FOR VIOLATING THE DISPOSAL RULE.** An employer’s failure to properly dispose of consumer information can result in substantial civil penalties. Individuals harmed by an employer’s *willful* failure to dispose of consumer information may recover actual damages or \$1,000, whichever is greater, plus costs and attorneys fees. Individuals harmed by an employer’s *negligent* failure to dispose of protected information may recover actual damages plus costs and attorneys fees. Federal and state authorities can also bring enforcement actions against employers that violate the Disposal Rule. If such an action is successful, the employer may be liable for actual damages for \$2,500 *per violation*, plus costs and attorneys fees.

Additionally, although the Rule does not require “proper disposal” of employee information that was *not* provided by a consumer reporting agency, employers should take care in disposing of such information. If an employer disposes of sensitive employee information in a negligent manner, (e.g., throws out an employment application containing the applicant’s name, address, date of birth, social security number, and driver’s license number without first shredding it), and the employer’s negligence results in the applicant’s identity being stolen, the employer could find itself dragged into litigation.

**What Should Employers Do?** To avoid potential liability, employers should implement written policies and procedures that require (1) the burning or shredding of documents that contain sensitive information about prospective and current employees, and (2) the destruction or erasure of electronic media that contains sensitive information about prospective or current employees. Employers should train employees regarding the policies and procedure, as well as monitor compliance with the policies and procedures. Instead of implementing and monitoring their own process, larger employers may prefer to contract with a reputable record destruction business to dispose of employee records that contain sensitive information. If an employer does so, it should monitor the contractor’s compliance with the Disposal Rule.

This Employment Law Note is written to inform our clients and friends of developments in labor and employment relations law. It is not intended nor should it be used as a substitute for specific legal advice or opinions since legal counsel may be given only in response to inquiries regarding particular factual situations.



***“We’re Going To Make Your Business Day Better!”***

**Renton 425-271-4225 // Seattle 206-223-4001 // Fife 253-922-6770**  
**[www.smarttalent.net](http://www.smarttalent.net)      [info@smarttalent.net](mailto:info@smarttalent.net)**

**Office - Accounting/Finance - Medical - Mortgage - Legal - Production - Warehouse - Professional  
Temporary - Temp-to-Hire - Direct Placement**

**100% Guarantee on Temp Assignments and up to a 1-Year Guarantee on Direct Placement**

---

---