

New Employer Obligation To Protect Employees And Applicants Against Identity Theft

As of June 1, 2005, employers will be required to "properly dispose" of "consumer information derived from consumer reports" to comply with new obligations under the Fair and Accurate Credit Transaction Act of 2003 (the "FACT Act") and the implementing regulations codified at 16 C.F.R. § 682 *et seq.*

Will Your Company Be Affected By The New Information Disposal Rule?

If your company uses an outside agency to conduct background checks or other employment investigations, it must comply with the new information disposal rule.

According to the new rule, any person (including any company) who maintains or possesses consumer information for a business purpose must comply with the new disposal standard. The regulations define "consumer information" as "any record about an individual, whether in paper, electronic or other form, that is a consumer report or is derived from a consumer report. Consumer information also means a compilation of such records." A consumer report is any written, oral or other communication of any information by a consumer reporting agency bearing on a consumer's credit, character, general reputation, personal characteristics or mode of living. Consumer reports include information obtained by employers from background checks and other employment investigations performed by outside agencies.

What Must Your Company Do To Comply?

The new rule requires companies to take "reasonable measures" to protect against unauthorized access to or use of the information in connection with its disposal. The broad definition of "disposal" includes not only the discarding of information, but also the "abandonment of consumer information" and "the sale, donation, or transfer of any medium, including computer equipment, upon which consumer information is stored."

Rather than requiring specific disposal methods, the regulations obliquely provide a list of examples of "reasonable measures", cautioning that they are "illustrative only" and are not exclusive or exhaustive compliance methods. The examples include:

- Implementing and monitoring compliance with policies and procedures that require the burning, pulverizing, or shredding of papers 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 so that the information cannot practicably be read or reconstructed; and
- Outsourcing the disposal of information to a record destruction company (such as a shredding company), so long as the employer (1) performs "due diligence" when selecting the record destruction company, and (2) enters into, and monitors compliance with, a contract requiring document destruction in a manner consistent with the FACT Act's implementing regulations. Although the regulations do not spell out what "due diligence" is required, they instruct that "due diligence could include" 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, 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."

The FACT Act Penalizes Willful & Negligent Failure, And Allows Attorneys' Fees

The implementing regulations provide that willful, and even negligent, failure to comply with the regulations could expose covered employers to civil liabilities and penalties, including actual damages, punitive damages (in the case of willful violations), and attorneys' fees and costs.

Other Laws Protecting Against Misuse Of Personal Information

The FACT Act's implementing regulations are just the latest in an expanding set of laws designed to protect applicants and employees (among others) from the misuse of personal information, including the following:

- **The Fair Credit Reporting Act ("FCRA") and State Consumer Reporting Laws.** FCRA requires employers to comply with certain procedural requirements, including use

of appropriate disclosure, authorization, certification and adverse action forms, before obtaining and using background checks and other consumer reports on applicants and employees. Several states, including California, also have their own consumer reporting laws, which impose additional obligations on employers who obtain and use consumer information about applicants and employees, even when the information is obtained through certain in-house investigations.

- **The California "Confidentiality of Social Security Numbers" law** prevents California employers from, among other things, publicly posting or displaying an individual's social security number, requiring an employee to use his or her social security number to access information or services, or printing an individual's social security number on any materials mailed to the individual.
- **California's Megan's Law** provides that registered sex offender information available through the new California Megan's law website may only be used to protect a person at risk. The law specifically prohibits the use of information from the website for employment purposes, and may even subject an employer to liability (including punitive damages and attorneys' fees) if it misuses the information obtained from the website. Other states also have sex offender registries and restrictions on employer use of such information.
- **California's Notification Law Regarding Security Breaches** requires employers to immediately notify the owners of personal information stored in the employer's computer system (including social security numbers and driver's license numbers) of any security breach if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person, unless a law enforcement agency determines that the notification would impede a criminal investigation.

Steps Your Company Should Take

To ensure compliance with the FACT Act's new regulations and other laws protecting against misuse of personal information, employers should:

- Review current practices and procedures regarding background checks and employee investigations; confirm compliance with FCRA and any applicable state laws, including sex offender registry laws.
- Review and/or implement procedures regarding the use, storage and protection of personal information of applicants and employees.
- Review and/or implement procedures to respond to security breaches and to provide any notice required under applicable state law.

- Review current practices regarding the disposal of paper documents, as well as the destruction or erasure of computers, disks or other electronic media containing employee information, and revise the practices as necessary to comply with the new information disposal rule.
- Train and monitor employees to ensure that they are following the company's established practices and procedures regarding personal information.

Please feel free to contact us with any questions about the new information disposal rule, or for assistance in navigating the growing list of laws regulating the gathering and use of personal information regarding current, former and prospective employees.

Miller Law Group is a Bay Area law firm that specializes in representing management in all facets of employment litigation and counseling. For more information about these new developments, or for general employment advice, please call Michele Ballard Miller, Maki Daijogo or Kristin Pedersen at (415) 464-4300 or e-mail us at mbm@millerlawgroup.com.

This information is a general description of the law and is not intended to provide specific legal advice.

Copyright © 2005 Miller Law Group. Permission is granted to make and redistribute, without charge, copies of this entire document provided that such copies are complete and unaltered and identify Miller Law Group as the author. All other rights reserved.

You received this e-mail because you are currently on our mailing list. If you wish to be removed from our list, please send a reply to this message with the word "unsubscribe" in the subject line, or complete [this form](#).