

ID Theft Case Law

Recent FTC Regulation and Case Law Development Require Reevaluation of Employee Data Storage

Related Areas: [Labor & Employment](#)

June 2005

Identity theft has become this country's primary fraud complaint. A prime target for identity theft is information collected by employers about employees, job applicants, customers or business partners.

It is virtually impossible to run a business without collecting personal, identifying information such as names, addresses, Social Security numbers, and credit card numbers. Indeed, many employers use background checks in their hiring processes which include an applicant's credit report, and virtually all employers maintain confidential employee personnel files. Employers have every right to collect information necessary to make hiring and business decisions, as long as they comply with federal and state laws regarding information collection. But employers also need to be careful about how they maintain that information to ensure compliance with applicable law and to guard against identity theft. A new Federal Trade Commission ("FTC") regulation and a recent court decision send a clear message to employers, requiring reevaluation of policies and procedures concerning the use, storage, safeguarding and disposal of identifying information.

FTC Issues New Regulation That Puts More Responsibility On Employers

Pursuant to the Fair and Accurate Credit Transactions Act of 2003 ("FACTA") and the Fair Credit Reporting Act ("FCRA"), the FTC adopted a regulation that imposes new requirements on employers that collect and store information about their employees, job applicants, customers and any other individuals with whom the employer conducts business. That regulation, which became effective June 1, 2005, requires employers (as well as any other entities or individuals) that use consumer reports to adopt "reasonable and appropriate" measures to dispose of sensitive information derived from such reports. The regulation applies to all information, regardless of how it is obtained or stored, whether in hard copy, electronically or by some other means. The FTC's definition of a consumer report is quite broad. It includes credit reports, credit scores, third party reports with information relating to employment background, reference checks, check writing history, insurance claims, residential/tenant history, or medical history.

The regulation stops short of dictating specific disposal methods, and instead requires that each employer adopt measures that are reasonable and appropriate to prevent unauthorized access to or use of sensitive personal information. The regulation is purposely flexible to allow employers to determine what measures are reasonable based on the sensitivity of the information, the costs and benefits of various disposal methods, and variations and changes in technology. While no particular means is prescribed, the FTC suggests that employers consider burning, pulverizing or shredding paper containing personal information, destroying or erasing electronic files, and conducting a comprehensive audit of information security policies and procedures. Although the new FTC regulation only applies to consumer reports, given that the information derived from such reports is likely transferred to other records and used in a multitude of ways, employers should take similar protective measures for any records containing personal or financial information of others, keeping in mind, of course, that some data must be preserved for specified time periods, as dictated by law.

With the FTC's recommendations as a guide, employers should review their current methods of information disposal to ensure that sensitive information is not just thrown out, but also destroyed or deleted. It is equally important for employers to reevaluate the types of information gathered from employees, job applicants, customers and others and determine what information is essential to the operation of the business. The less sensitive information employers unnecessarily gather, the easier it is for employers to monitor and safeguard the use, storage and disposal of the information. Employers should develop comprehensive records retention and information security policies outlining usage, safeguarding and disposal measures to be taken by the employer, and communicate these policies to all users and providers of personal information.

Court Declares That Custodians Of Employee Information Have Duty To Safeguard That Information

Just before the FTC regulation took effect, a Michigan court gave employers another reason to reevaluate the manner in which information about employees is gathered and stored. In February 2005, the Michigan Court of Appeals became the first court in the country to find that custodians of employee information have a duty to guard the data with the "utmost care."

In *Bell v. Michigan Council 25 AFSCME*, a group of 911 operators for the City of Detroit sued their union for negligence when they became victims of identity theft. The treasurer of the union had been allowed to take home reports that included employee job classification information, Social Security numbers and other personal information. The treasurer's daughter obtained that information (a notebook was found in her bedroom containing members' names, Social Security numbers, driver's license numbers) and used the information to obtain illegal phone services and purchase various other items in the employees' names. A jury found that the treasurer's daughter had stolen the employees' information from her mother (the union treasurer) and used the information to commit identity theft.

The union argued that it was not liable for the unforeseeable criminal acts of a third party, but the court strongly disagreed. The court found that when a "special relationship" exists between the victim of criminal conduct and the person whose negligence allowed or contributed to the commission of the crime, that person can be found liable for the criminal conduct. The union, in the court's view, had a special relationship with the employees (its members) and therefore had a duty to safeguard its members' private information. The members had entrusted their personal information to the union and had a right to expect that the information divulged in confidence would be guarded with the utmost care.

Although the union was not an "employer" in this case, the analysis is applicable to employers. Employers and their employees, job applicants, business partners and customers have a special relationship, one in which vast amounts of personal, identifying information is exchanged. This case presents a sobering warning to employers that they must be very careful when it comes to the use, storage and disposal of the personal information of employees and others with whom they have a business relationship. Employers must securely guard the personal information of their employees, job applicants, customers and clients. Records and files that include personal information should be stored in locked areas or password-protected databases and should not be allowed to leave the employer's premises, except in certain limited circumstances. And when such information is permitted to leave, it is critical that the employer have a solid policy in place concerning how this information is protected while off-site.

Courts Are Not The Only Ones Paying Attention

State legislatures also are beginning to pay attention to the rise in identity theft and increasingly are passing legislation to protect personal information. This year, Michigan became the first state to enact legislation requiring employers to maintain a privacy policy to safeguard employee Social Security numbers. Virginia recently followed suit. Several states, including Arizona, California, Illinois, New York, and Texas, are considering enacting or have already enacted legislation that mandates stronger protection of personal information, particularly Social Security numbers. It is just a matter of time before this type of legislation becomes commonplace.

What Can Employers Do To Protect Themselves?

Employers would be prudent to implement comprehensive information protection now to limit their exposure to liability and to avoid being "the first" (as was the case with the union in *Bell*). Among other things, employers should:

- Review how and when employee or job applicant Social Security numbers are used, especially when used in conjunction with other information like names and addresses. Consider using alternative identification descriptors, like randomly assigned identification numbers, that could replace the use of Social Security numbers as workplace identifiers.
- Audit personal employee information currently maintained, and determine if all data elements are absolutely essential for business or government reporting purposes. Eliminate any data that is not essential or is merely "nice to have."

- Review employment application and other forms. Consider eliminating requests for information that are not absolutely essential or not necessary for evaluation or other background checks.
- Keep all employee and applicant records in locked and secure areas. Individuals with access to such records should be clearly identified and responsibilities for maintaining the security of these records should be specifically assigned.
- Consider instituting criminal/credit background checks for all employees who have access to sensitive employee information.
- Develop and communicate:
 - a records retention policy that outlines what types of records will be maintained, for what purposes they will be used, what safeguards have been put in place to ensure adequate protection of personal information, and what procedure will be followed to properly destroy the records at the end of the retention period.
 - an off-site policy that prescribes the limited circumstances under which information may be used off-site, procedures for removing sensitive information from company premises, and means of safeguarding information while used at off-site locations. Institute a strict authorization procedure to be followed before any information is taken off-site and communicate the consequences for misuse or security breaches while information is being used off-site.
 - a laptop computer usage policy that delineates when and how laptop computers are to be used. Develop a password-protected system by which only the person specifically authorized to use a laptop may log into that particular computer and instruct users on how to lock the computer when not in use.
- Require all personnel with access to any portion of your information system, including electronic mail, voice mail, and computer databases, as well as anyone who is authorized to use company computers, to have a login and password that is specifically assigned to that person. Remind users to keep login information confidential.

* * * * *

Implementing a comprehensive protection and disposal policy for personal identifying information may be time-consuming and tedious. However, such a policy can significantly reduce potential liability. Should you have any questions about your particular processes, please contact