ASAP™

A Littler Mendelson **Time Sensitive** Newsletter

in this issue:

JUNE 2005

Effective June 1, 2005, the new regulations require employers to take reasonable steps to prevent unauthorized use of and access to consumer information during disposal of such information.

New FTC Regulations On Proper Destruction of "Consumer Information": Steps Employers Need to Take to Comply

By Philip L. Gordon and Cathy S. Beyda

As part of its comprehensive efforts to combat identity theft, the Federal Trade Commission (FTC) has promulgated regulations effective June 1, 2005 for the proper destruction of "consumer information." While some commentators have raised alarms by asserting that these new regulations create the potential for significant employer liability, and even class action lawsuits, the relatively limited scope of the regulations makes the practical reality of such liability more remote than the alarmist commentators suggest.

Requirements and Implications of the Disposal Rule

Because the new FTC regulations are limited to requiring the proper disposal of "consumer information," they have been referred to as "the Disposal Rule." Consumer information includes (a) consumer reports and (b) information derived from consumer reports, provided that the information is individually identifiable. As applied to the employment context, "consumer information" would include not only a background check report obtained from a consumer reporting agency but also, for example, notes prepared by a supervisor or human resources manager based upon information contained in the report. "Consumer information" encompasses information in both paper and electronic form.

The regulations require employers to take reasonable steps to prevent unauthorized use of, or access to, consumer information during the disposal process. While the regulations do not require any specific disposal methods, the regulations provide examples of the types of disposal processes that would be reasonable. Paper documents containing consumer information, for example, could be placed in locked trash bins while awaiting disposal and then shredded or burned.

"Disposal," when applied to consumer information stored on electronic media, encompasses not only tossing hardware, floppy disks, and CDs into a dumpster, but also the sale, donation and other transfer of the storage media. The regulations suggest that it would be reasonable for an employer to develop procedures to render electronically stored consumer information irretrievable before disposal. Employees, for example, could be required to magnetically swipe disks, or scratch CDs, containing consumer information before disposing of them. Employers also could consider the reasonableness of having appropriately trained personnel check all hard drives containing consumer information before the computers containing those hard drives permanently leave the employer's premises — whether for donation to a school, for sale by a second-hand computer warehouse, or for incineration by the municipal waste department.

While not specifically required by the regulations, the FTC suggests that businesses relying on third parties for the disposal of records containing consumer information should engage in due diligence before selecting, or continuing to use, a disposal company. Examples of "due diligence" contained in the regulations include obtaining several references for the disposal company, requiring the company to produce a certification by a trade association or other third party that has reviewed the disposal company's information security policies, or reviewing an independent audit of the company's disposal methods.

Although the regulations apply only to the process of destroying consumer information, compliance with the regulations is likely to involve the establishment of polices and procedures governing the disposal of

information as well as appropriate employee training. It is important to note that neither the FCRA nor the new regulations creates document retention periods. Accordingly, employers must look elsewhere when deciding how long to retain records containing consumer information.

The state anti-discrimination statutes provide some guidance in this regard. Depending on the state, these statutes often require employers to maintain records relating to the hiring process for 2 years or more. When a claim of discrimination has been brought, however, most states require that relevant documents be retained until final disposition of the claim.

Other state laws also should be considered. For example, in Oregon, employers are required to maintain records used in determining a person's qualifications for employment, promotion, etc. for at least 60 days after termination of the employment. In addition, the state statutes of limitation governing the time period in which a person may bring an administrative or court claim for discriminatory failure to hire may be relevant, and commonly range from two to six years after the adverse employment action was taken. Developing an appropriate record retention policy is essential. Because a variety of different statutes and issues must be considered when doing so, however, employers are advised to consult qualified employment counsel for assistance with this endeavor.

Potential Employer Liability

The FTC promulgated the new regulations in order to enforce Section 216 of the FACT Act, which, in turn, amends the Fair Credit Reporting Act (FCRA). The reader can find more information regarding the impact of the Fact Act on employers in Littler's ASAP, *The FACT and How it Affects FCRA and Employment Investigations (the Vail Letter)*, available at http://www.littler.com/nwsltr/asap_01_FACT.html.

Because the new regulations are promulgated under the FCRA as amended by the FACT Act, employers who do not comply with these regulations, and whose employees or job applicants ultimately are victimized by identity theft as a result, could face a lawsuit seeking to enforce the remedies authorized by the FCRA. In the case of negligent violations, FCRA remedies are limited to actual damages and an award of attorneys fees and costs. Willful violators may be subject to statutory damages of up to $1,000 per violation or to an award of actual damages, whichever is greater, and may be required to pay a prevailing plaintiff's attorney's fees and costs.

Conclusion

All employers who possess or maintain consumer information must begin to develop reasonable measures to dispose of such information in order to protect against the unauthorized access or use of the information. Careful consideration of an employer's unique circumstances in developing a disposal program should help to reduce the potential for identity theft as well as to minimize potential employer liability. Thus, while the need for immediate action is clear, the recent alarm surrounding the new regulations clearly is unwarranted.

Philip Gordon is a shareholder in Littler Mendelson's Denver Office, and Cathy S. Beyda is Special Counsel in Littler Mendelson's San Jose Office. If you would like further information, please contact your Littler attorney at 1.888.Littler, info@littler.com, or Mr. Gordon at pgordon@littler.com, or Ms. Beyda at cbeyda@littler.com.