February 2013

CIRSA HAZARD ALERT

Published by the CIRSA Loss Control Department | Your Partner in Risk Management

Identity Theft at the Workplace

Identity theft affects public entities in several ways. Not only can entities suffer direct loss due to this crime but inadequate security and lax business practices may open up an entity to lawsuits, fines, and adverse publicity.

The federal Fair and Accurate Credit Transactions Act (FACTA) of 2003 says employers that negligently or purposely let employees' personally identifiable data fall into the wrong hands can face fines of up to $2,500 per infraction.

Identity theft occurs when unauthorized persons gain access to and use another person's personal information such as his or her name, Social Security number, credit card, bank account number, or other identifying information to commit fraud or other crimes. Identity thieves gain access to personal information through a variety of sources such as lost or stolen credit cards, stolen paper mail, dumpster-diving, computer spyware or hacking, e-mail scam, or by accessing customer or employee records. Instances of identity theft have increased dramatically over the last several years. In fact, according to the United States Federal Trade Commission (FTC), in 2011 identity theft was the nation's top consumer complaint for the twelfth year in a row. In 2011 alone, approximately 11.6 million adults became victims of identity fraud in the United States, at a cost to the economy of approximately $54 billion. Because many instances of identity theft go unreported, the numbers are likely even higher.

Controlling the growing threat of identity theft presents significant challenges for employers. The vast amount of sensitive personal information maintained by employers about their employees, including demographic information, personnel files, background reports, Social Security numbers, benefits data, and payroll and tax records, can be a virtual treasure trove for identity thieves.

Strategies for Minimizing Identity Theft

- Develop a comprehensive information security policy that includes responsible information-handling practices for employees, customers, and other sensitive business records.
- Restrict access to sensitive information to only those employees with a "need to know".
- Train employees with access to sensitive information on how to keep it secure.
- Disable employee access to entity records and computers immediately upon termination.
- Do not use Social Security numbers as an employee identifier.
- Consult with the entity's counsel to discuss federal and state requirements concerning the handling of employee information and for assistance in implementing comprehensive information security policies, procedures, and contingency plans.
- Consider conducting background checks for candidates and current employees who handle or have access to sensitive and confidential information.

(continued on back)

Identity Theft at the Workplace (cont.)

- Review your entity's records retention policy to ensure all types of sensitive records are addressed.
- Don't cover up breaches. Work with law enforcement to facilitate prompt disclosure to affected individuals.
- Implement a data-removal policy that limits who can take sensitive information from your premises and how they must secure it. It's best to make sure employee data stay within your walls. But if you do allow employees to remove personal data—say on laptops—make sure to password-protect and encrypt the data.
- Implement a lost/stolen equipment policy for laptops, iPads, flashdrives, and other mobile devices.
- Secure job applications which contain sensitive information. Store paper applications in a locked area with limited access. Receive applications over the Internet only through encrypted web pages.
- Destroy old computer hard drives that contain sensitive information. Use a certified company who will issue a letter of authenticity of equipment destruction.

Although no entity can keep its records entirely secure from identity theft, adopting these strategies can help to protect employees to minimize a municipality's exposure from this growing threat.

ID theft online resources:

FACTA information: www.privacyrights.org/fs/fs6a-facta.htm

State laws: www.ncsl.org/?tabid=12538