IRELAND STAPLETON

Safeguarding Employee Records from Identity Theft

Identity theft is terrifying. The idea of someone using your information – Social Security numbers, addresses, etc. – to conduct business or move assets strikes fear in the heart of many. Reclaiming a lost identity is exhausting, time consuming and expensive. For example, a survey prepared for the Federal Trade Commission found that 16 percent of victims of identity theft polled had to pay for some or all of the identity's thief's purchases. According to the survey, victims spend an average of 81 hours trying to undo the damage, and 28 percent of those polled had been unable to restore their identity despite spending more than a year trying to do so. How does this stress impact the workplace? HR records contain sensitive information, and its protection is of paramount importance. Social Security numbers, birthdates, the identity of family members, health information and other details provide fertile ground for hands-on and cyber identity thieves.

What can you do to protect your employees and your company from identity theft? Look at how and when you use employee Social Security numbers, especially when coupled with other information, i.e., name and address. In most situations, alternative identification descriptors could replace the use of SSNs. Pay particular attention to the use and storage of financial and HR systems and company intranets, as these systems are subject to attack by cyber villains. Review job descriptions and confirm which employees must have access to sensitive employee records information. Consider conducting ongoing background checks for those employees. 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." Shred outdated hard copy records that contain confidential employee information. And, by all means lock and secure all employee and applicant records and allow access only to those with a need to know.

What should you do if you become aware that sensitive employee information has been made available to employees who are not authorized to have it? The increase in identity theft crimes has resulted in the enactment of numerous state security breach notification laws. These laws generally do not distinguish between consumers and employees. Consequently, employers are wise to comply with these laws in the event that employee personal information is acquired by unauthorized individuals.

IRELAND STAPLETON

Colorado has a statute that governs an employer's responsibilities in the event of a breach of security regarding employees' personal information. This statute, C.R.S. § 6-1-716, is part of the Colorado Consumer Protection Act, and applies to incidents occurring on or after June 1, 2007. The statute provides that in the event of a breach of the security of the system, an employer must conduct a good faith investigation to determine the likelihood that personal information has been or will be misused. Unless the investigation determines that no such misuse has occurred or is likely to occur, the employer must notify the affected employees.

For example, say your HR professional sends an email to the entire company and mistakenly attaches a document listing the names and Social Security numbers of all company employees. He or she immediately realizes the mistake and recalls the message. Although the message may only have been available for a matter of seconds, and you determine identify theft is unlikely to occur, best practices suggest that you notify your employees, explain the mistake, and direct them to resources on how to put fraud alerts on their credit.

From this discussion, take away one thing: An ounce of prevention is worth a pound of cure with issues of sensitive information and identity theft.

Laura J. Hazen is a director at the Denver-based law firm, Ireland Stapleton Pryor & Pascoe, PC. In her employment practice, Hazen provides day-to-day advice and coaching to public and private companies on various employment matters. She also has an active litigation practice where she concentrates on representing business in all aspects of complex business and employment disputes. You can contact her by email at lhazen@irelandstapleton.com or by phone at 303-623-2700.