ASAP™

A Littler Mendelson **Time Sensitive** Newsletter

in this issue:

APRIL 2005

With identity theft on the rise, Michigan becomes the first state to enact legislation requiring that every employer maintain a policy for safeguarding employee social security numbers. During the same time frame, a Michigan Court of Appeals became the first appellate court to allow the victims of identity theft to recover damages from an organization that failed to adequately safeguard personal information that was subsequently used for identity theft.

Michigan Becomes the First State in the Nation to Open the Door to Potential Employer Liability for Workplace Identity Theft

By: Philip L. Gordon, Esq., and Jeffrey Davis, Esq.

In early 2005, Michigan became the first state in the nation to enact legislation requiring that every employer maintain a policy for safeguarding employee social security numbers. During the same time frame, the Michigan Court of Appeals became the first appellate court to allow the victims of identity theft to recover damages (totaling $275,000) from an organization that failed to adequately safeguard personal information that was subsequently used for identity theft. These national precedents expose Michigan employers to liability for failing to safeguard employee personal information, and open the door to employer liability for workplace identity theft in other jurisdictions that likely will follow Michigan's example.

Michigan Enacts the First Statute Mandating a Policy to Protect Employee SSNs

Section 4 of Michigan's Social Security Number Privacy Act ("the Act"), Mich. Comp. Laws Ann. §445.84 (West 2005), which went into effect on March 1, 2005, is the first statute in the nation to require employers to adopt a policy to protect the confidentiality of employee social security numbers ("SSNs"). The Act was just one of eleven pieces of legislation enacted by Michigan in late 2004 to combat identity theft.

The Act requires employers, and any other entity that collects SSNs of more than one individual in the ordinary course of business, to establish a policy that:

- ensures to the extent practicable the confidentiality of SSNs;
- prohibits unlawful disclosure of SSNs;
- limits who has access to information or documents containing SSNs;
- establishes a document destruction protocol; and
- requires the imposition of penalties on those who violate the policy.

The policy must be implemented on or before January 1, 2006.

The statute leaves no doubt that it is aimed at employers not only because all employers collects SSNs from employees in the ordinary course of business, but also because the statute requires publication of the policy in an employee handbook, or in other similar documents. The statute does not proscribe the means of publication. Consequently, employers may choose to satisfy the statutory requirement by posting the policy on their website or intranet.

Michigan Court of Appeals Affirms $275,000 Verdict Against Union Whose Stolen Membership Information Was Used to Commit Identity Theft

In an unprecedented decision, *Bell v. Michigan Council 25 AFSCME*, the Michigan Court of Appeals, with one judge dissenting, affirmed a $275,000 jury verdict against a union whose members were victimized by identity theft. In that case, the union's treasurer brought home documents containing the name and social security number of union members. The jury found that the treasurer's daughter had stolen the information and used it to perpetrate identity theft against the thirteen union members who were plaintiffs. The jury determined that the union was negligent in failing to adequately safeguard the personal information from theft by the treasurer's daughter.

On appeal, the union sought reversal of the jury's verdict by invoking the general rule that a defendant in a negligence action is not legally responsible for the unforeseeable criminal acts of a third party. This general rule, however, does not apply in Michigan (or in many other jurisdictions) when a "special relationship" exists between the victim of the criminal conduct and the defendant whose negligence allegedly permitted commission of the crime. The appeals court noted that whether such a special relationship exists is a fact-intensive question that must be decided on a case-by-case basis.

The appeals court found the necessary special relationship based on several factors. First, because the union was the legal representative of the union members who were plaintiffs, the union had an obligation to act in the plaintiffs' best interests by safeguarding their personal information. Second, the union was in a better position than its members to control access to the personal information used to commit identity theft. Third, the risk to sensitive information stored in an unsecured environment, *i.e.*, the treasurer's home, was foreseeable because of the increasingly prevalent threat of identity theft. Fourth, the severity of the potential harm was substantial given that identity theft can result in significant monetary losses and damage to creditworthiness. Finally, the burden on the union to safeguard the information was not substantial, yet the union had required no safeguards for the documents taken to the treasurer's home even though the possibility of identity theft was "far too commonplace."

Implications of Developments in Michigan for Employers

Michigan's Social Security Number Act and the Michigan Court of Appeals' decision in the *Bell* case open the door to potential employer liability for work-related identity theft. Most of the factors upon which the Michigan Court of Appeals relied in finding the necessary "special relationship" between the union and the victims likely will be present whenever an employer fails to provide adequate safeguards for employee personal information, whether that information is taken home or not adequately protected at work.

One material distinction between the circumstances in *Bell* and the stealing of employee personal information that results in identity theft is that unlike unions, employers generally do not have a duty to act in the best interests of their employees absent a statutory mandate to do so. Michigan's Social Security Number Act, however, most likely would vitiate this distinction. The Act could be construed to create the type of duty with respect to safeguarding social security numbers that would support a court's finding of the special relationship necessary to impose liability on an employer for identity theft perpetrated by a third person.

These developments in Michigan have broader implications for employers nationally. More than one-half dozen states, including Arizona, California, Illinois, and Texas, have enacted statutes that impose duties on employers to restrict the use and disclosure of SSNs. While these statutes do not require a policy that is as broad as Michigan's Social Security Number Act, they still impose restrictions that a court might cite in support of a finding that a "special relationship" existed between the employer and an employee whose SSN is stolen from the employer and then used by a third party to commit identity theft. Even in jurisdictions without statutes specifically restricting an employer's use and disclosure of employee SSNs, the tide of legislation focused on identity theft and the safeguarding of SSNs coupled with the other factors identified in the *Bell* case, might be viewed as sufficient to support a finding of the necessary "special relationship."

In light of these developments, all employers should consider implementing a policy similar to the one that Michigan employers are required to implement by January 1, 2006. Doing so will involve more than paying lip service to the elements listed in Section 4 of Michigan's Social Security Number Act. For example, issuing a policy stating that documents containing SSNs must be properly destroyed will not suffice. Instead, employers should detail how the proper destruction will be effectuated.

By way of illustration, the policy should explain that employees with access to paper documents containing SSNs must shred those documents when discarding them or place them in a locked trash bin the contents of which will be shredded. In addition, a single person or group within the information technology (IT) department should be responsible for ensuring that SSNs in electronic storage are rendered irretrievable before the equipment is discarded. Limiting access to SSNs, ensuring their confidentiality, and preventing their unlawful disclosure will similarly require more than policy statements in an employee handbook to be effective.

Conclusion

All employers should implement the type of privacy policy that Michigan employers are required to adopt. Adopting such a policy and making sure that the policy is followed will go a long way towards reducing the risk of a costly jury verdict in favor of employees whose SSNs were stolen and used by a third person to commit identity theft.

Philip Gordon is a shareholder, and Jeffrey Davis is an Associate, in Littler Mendelson's Denver 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 Mr. Davis at jfdavis@littler.com.