

Identity Theft and Employer Liability

by Guillaume Deybach

The Federal Bureau of Investigation calls identity theft an "increasingly insidious and pervasive problem" that can threaten virtually anyone. More ominously, identity theft "costs American businesses and consumers a reported \$50 billion a year, causes untold headaches for an estimated 10 million U.S. victims annually, and even makes it easier for terrorists and spies to launch attacks against our nation."

As identity theft continues to grow as a crime and a social, financial and security concern, questions of liability become more crucial. In light of the criminal and social considerations, the litigious environment of the United States, and existing and emerging laws concerning corporate responsibility for the protection of personal data, commercial entities have begun to take actions of their own to protect the data of their customers and, increasingly, their employees.

A closer examination of the personal impact of identity theft reveals why it is a growing concern among corporate risk managers. Consider this scenario: An employee of an American company is sent to Monterrey, Mexico, by her company to study the capabilities of an IT service provider. While in Monterrey, she uses her company credit card to pay for her hotel, food and local transportation expenses. She also uses a personal credit card to purchase some gifts for her family back home. Her business in Mexico completed, she returns to the United States.

One month later, her credit card bills arrive and sit on her home desk for two weeks until she makes the time to address them. As she scans the charges from her trip—now six weeks in the past—she notes a \$50 charge from a Monterrey financial institution with a name that she does not recognize. Her personal credit card company advises her it is probably just a processing transaction related to a purchase from her recent trip and agrees to reverse the charge. She then pays the bill and gets on with her busy life. On her next personal credit card statement, four mysterious charges from various Caribbean islands appear totaling \$800 dollars. Ten weeks after her trip to Mexico, she comes to terms with the fact that her identity has been stolen.

In this scenario, our hypothetical victim is fortunate. Her potential losses are only in the hundreds of dollars, and it took her less than three months to discover the theft. A more common scenario would involve thousands of dollars and possibly take six months to discover. More alarmingly, a typical identity theft victim can spend up to 600 hours to resolve a single case of identity theft over the course of a year, according to a survey conducted by the nonprofit Identity Theft Resource Center.

The customer service required to help consumers resolve issues related to identity theft is fairly sophisticated. Subsequently, many credit card companies and credit reporting agencies cannot provide these high-level services on a 24/7 basis. So individuals often must take time during the workday to resolve these issues. This reality creates a connection between identity theft and employee productivity. Given the FBI's estimate of 10 million U.S. identity theft victims each year and the workday time each of them will likely spend resolving this victimization, the potential productivity losses become significant. Productivity losses, however, are not the only concern related to identity theft among corporate risk managers.

An Inside Job

Personal data losses occur in a number of ways. Personal information can be stolen via the Internet when online transactions are made. Identity theft can also occur when there is some kind of personal connection between the thieves and their victims. For employers, a more critical concern is when identity theft can be tied to the action of employees, which one recent study said accounted for some 16% of identity theft cases.

Perhaps the best known case involved the loss of up to 26 million personal records from the U.S. Department of Veterans Affairs due to an employee improperly taking the records home on a laptop computer, which was subsequently stolen. Other cases involving other government agencies include the U.S. Census Bureau and the National Oceanic and Atmospheric Administration (NOAA). Private sector organizations that recently experienced data breaches at the hands of employees include Bank of America, Fidelity Investments, LexisNexis and DSW Shoe Warehouse. When employees mishandle personal data and losses occur, employer-whether private or public sector-are culpable.

A groundbreaking case in Michigan provides a sobering illustration of this culpability. Last year, Michigan became the first state to require by law that every employer establish a policy for keeping employee social security numbers safe. The law was passed at nearly the same time a Michigan appeals court allowed victims of identity theft to recover financial damages from organizations that did not adequately protect personal data that were subsequently used for identity theft. In the court case, a labor union employee took home documents showing union members' names and social security numbers; the employee's daughter stole the information and used it to engage in identity theft. The union was found liable for the actions of its employee.

Undeniably, corporations have increasing liability for the security of employee and customer information and personal data, and a justified concern for protecting all parties from this rising risk. An increase in security breaches involving lost or stolen personal data has accentuated the need for a solution, leading to lawsuits and the implementation of related laws and regulations across the country.

A Flurry of Activity

In addition to the above events in Michigan, a number of other data-protection initiatives have been keeping legislators busy in Washington and in state capitals around the nation.

California was the first state to pass a law requiring notification of all affected parties when a data security breach has occurred involving their personal information. According to the National Conference of State Legislatures (NCSL), similar legislation

was introduced in 31 states during 2006 and has already been enacted in at least 12 states. NCSL also says that 38 states have introduced legislation aimed specifically at protecting social security numbers (as in Michigan). The Information Technology Industry Council (ITIC) is calling for a federal breach notification law to preempt myriad state laws with varying requirements. ITIC is also calling for federal laws that go beyond breach notification to promoting industry-wide best practices that reduce the risk of breaches and provide harsh penalties for intentional acts of identity theft.

In short, all three branches of government, at both the state and federal levels, are focused on identity theft to some degree. The net result will be increased statutory, regulatory and legal pressure on corporations to protect personal data and to protect their businesses from subsequent financial and productivity losses.

A Tall Order

So what must corporations and their risk managers consider when developing their data protection/identity theft strategies?

The list is significant:

- What types of policies must corporations implement to ensure that customer and employee data remains protected?
- What types of protocols and procedures must be in place to minimize risks related to employee actions that lead to data security breaches?
- What alerting systems can be established to identify breaches as early as possible?
- How will breach notifications be handled so they comply with extant and emerging laws?
- How can the exposure of customer and employee social security numbers be minimized?
- What can be done to maintain appropriate levels of productivity among employees who have become victims of identity theft?

The answers will likely involve audits determining which employees have access to which data and why, enacting stricter pre-employment background checks, creating document destruction policies and procedures, and maintaining employee education programs, to name a few.

A Nagging Issue of Productivity

While many of the above initiatives must be viewed by employers as important business activities, one issue emerges as a potential "third rail" of an unwieldy exposure, the impact of which is as potentially staggering as it is difficult to manage. That is, how can companies manage productivity losses related to employees who themselves have become identity theft victims?

Each individual employee victimized will likely spend significant work-time hours over the course of a year resolving issues related to identity theft, given that this is when most credit card companies and credit reporting agencies offer customer service. Assuming an employee minimizes work time spent on such matters-keeping time spent to only a couple of hours per week and under 100 hours for the year-this

would represent a 5% productivity loss for an employee working 40 hours per week.

The potential costs of these productivity losses can be staggering, especially when considered along with related regulatory compliance costs and potential legal liabilities. While the compliance costs likely lie in the realm of the COO and the potential legal liabilities are the concern of the general counsel, the risk manager may well be the executive called upon to mitigate the kinds of productivity losses discussed here.

A Daunting Task

Chances are, any one of us knows at least a few people who have been victimized by identity theft. Among working Americans, it is likely that one in 10 people have had their identities stolen. The financial losses notwithstanding, restoration of a person's good name and credit is a daunting task. Additionally, the companies those individuals work for are becoming increasingly culpable in the estimated 10 million cases of identity theft that occur in the United States each year. And authorities consider the threat to be one that will continue to grow.

Many of the corporate risks associated with identity theft can be mitigated by the development and implementation of sound policies, systems and procedures. Others will ultimately become matters for the courts. Those risks that flow from the affected individual, however, must be managed using available tools and products that both support the individual and protect the employer. In the absence of a solid risk management plan for identity theft, the potential losses are nearly unlimited.

***Guillaume Deybach** is the president and CEO of Worldwide Assistance, which offers identity theft resolution services, travel assistance, emergency medical evacuation and repatriation, medical referrals, case monitoring and international claims management.*

Reprinted from Risk Management Magazine.

Copyright Risk and Insurance Management Society, Inc. All rights reserved.