This article recently appeared in the *New York Law Journal*, December 15, 2003.

Incidence of Workplace Identity Theft Signals Need for Proactive Measures

by Terri M. Solomon, Philip L. Gordon and Leslie J. New

A clerical worker at the New York State Insurance Fund allegedly gained access to personal data of thousands of individuals, including other employees, and allegedly used that information to fraudulently obtain credit and goods.[1]

A hacker obtained unauthorized access to the State of California's entire employee database, containing sensitive information on more than 250,000 public employees.[2]

Employees at Ligand Pharmaceuticals, Inc., were victimized after a co-employee found a box containing personnel files allegedly stored in an unsecure area.[3]

WHILE identity theft typically conjures images of an anonymous hacker raiding a retailer's customer database, these scenarios demonstrate that employers and their work force are increasingly coming under attack from both insiders and outsiders. This development is not surprising: Employers, who routinely collect basic identifying information for each employee, house a potential treasure trove for identity thieves. This article will describe employers' potential exposure to employees when that treasure trove is looted and used by identity thieves, and then will discuss the proactive steps employers can take to reduce their exposure.

Extent of Problem

Identity theft occurs when a person without authority obtains the personal identifying information of another [name, social security number, date of birth, home address, etc.] and then commits fraud by, for example, taking out a loan, purchasing merchandise, or acquiring a credit card in the victim's name. A report issued by the Federal Trade Commission [FTC] in September 2003 reveals the magnitude of the crime.[4] In the 12 months preceding September 2003, almost 10 million cases were reported. These crimes caused nearly $50 billion in losses to businesses and financial institutions. The median out-of-pocket loss per incident was $500 to $1,000, and victims spent 15 to 60 hours, on average, trying to reverse damaged credit histories and fraudulent credit card charges.[5]

The precise impact of identity theft on the workplace is difficult to measure, but two statistics suggest that the incidence of identity theft at work is substantial. First, 14 percent of respondents to the FTC survey stated that they were victimized by a family member or a workplace associate.[6] Even if only half of

[1] "New California Law Blocks Debt Collections from Debtors who are Victims of ID Theft," The Bureau of National Affairs, Inc., Sept. 23, 2003, at 2152.

[2] Taylor C. Young, "California Disclosure Law Reaches out to Touch Arizona," The Phoenix Business Journal, posted at www.bizjournals.com [last visited on Nov. 21, 2003].

[3] Stephanie Amour, "Employment Records Prove Ripe Source For Identity Theft," posted at www.USAToday.com [last visited Nov. 17, 2003].

[4] Identity Theft Survey Report, Federal Trade Commission, posted at www.ftc.gov/os/2003/09/timelinereport.pdf [last visited Nov. 17, 2003].

[5] Id. at 7, 41.

[6] Id. at 31.

these respondents were victimized at work, that percentage would amount to 700,000 incidents of workplace identity theft in just 12 months' time. Second, a 2002 report by Transunion, one of the three major credit bureaus, suggests that this figure understates the problem. According to the Transunion report, theft of records from employers is one of the leading causes of identity theft.[7]

Exposure to Liability

While the damage to an employer from the unauthorized taking of personnel data could be significant, liability for the damage caused to individual employees when that information is used for fraudulent purposes poses an even greater risk.

With the median cost per victim ranging between $500 and $1,000, and the potential for hundreds, thousands, and even tens of thousands of employee-victims as sensitive personnel information increasingly is consolidated in centralized human resources information management systems, an employer's exposure where employees' identities are victimized at work could conceivably climb into the millions, not to mention the imputed cost of employee time spent trying to reverse the damage caused by the identity thieves. Surprisingly, no published decision has yet resulted in an employer paying damages to employees victimized by identity theft. Nonetheless, the legal underpinnings for such claims already appear to be in place.

Claims for negligent hiring, retention and supervision, used successfully in some states to hold employers responsible for workplace violence and other tortious conduct by miscreant employees, could provide one avenue of recovery. Under these theories of recovery, the employee-victims would be required to prove that the employer knew, or should have known, that the co-worker posed a risk of identity theft. However, this standard might not be too difficult to meet when the employer has authorized the perpetrator's access to sensitive personnel information -- for example, by providing a temporary clerical worker with access codes to perform data entry in a human resources information system, or by outsourcing benefits administration without scrutinizing the "bona fides" of the outsourcer and its work force.

Even if the employer had no reason to know that the perpetrator might engage in identity theft, for example, in the case of a hacker, the employer still could face liability for negligence in a lawsuit filed by victimized employees. More and more federal and state statutes and regulations are setting standards for protecting sensitive data. While these standards often do not support a private right of action, they do create a legal duty, enforceable through a claim for negligence or under other legal theories.

Regulations promulgated under the Health Insurance Portability and Accountability Act of 1996 [HIPAA], for example, require employers administering group health plans to establish adequate physical, technical and administrative safeguards for protected health information.[8] The State of Washington has enacted legislation regulating the destruction of employee financial and health information.[9] California law imposes strict limitations, applicable to employers, on the display, mailing, and electronic transmission of social security numbers.[10] A bill modeled after this California legislation, the Privacy Act of 2003, currently is pending in Congress.[11]

The tort known as "unreasonable disclosure of private facts" may be a viable theory of recovery when the employer itself authorized the disclosure of personal information, and the disclosure resulted in identity theft. By way of illustration, *Bodah v. Lakeville Motor Express, Inc.*[12] was a putative class action filed by employees of a trucking company after discovering that the company's safety director sent a facsimile containing the social security numbers of more than 200 employees without taking precautions to protect the confidentiality of the fax. Significantly, the Minnesota Supreme Court unequivocally recognized that the social security number is a private fact whose unreasonable disclosure could support a claim. The court ordered the case dismissed only because the plaintiff employees had failed to allege sufficiently broad publication of the numbers.

Best Practices

The theories of employer liability for identity theft discussed above share a common thread. While the employer should be able to defeat each of these theories on a variety of grounds, the best defense is one which would prevent the lawsuit from being filed in the first place. To that end, the employer should consider implementing the proactive approach to preventing identity theft by taking the four measures discussed below: establishing a data protection/privacy policy, controlling access to sensitive data, implementing physical and technical safeguards, and training the work force. In addition to reducing potential exposure, implementing these measures can be a means of improving employee morale and building employee trust and loyalty by demonstrating the employer's concern for the security and privacy of employees' personal information.

Establishing a Data Protection/Privacy Policy. The data protection/privacy policy should embody all aspects of the employer's efforts to reduce the risk of liability from identity theft. The policy should identify the circumstances in which sensitive data may be collected from job applicants and employees, the types of data to be collected, and how the employer may use and disclose the data.

The policy should strictly limit the collection, use and disclosure of sensitive data to the minimum necessary for the intended purpose and eliminate all unnecessary collection, uses and disclosures. For example, social security numbers should not be requested from job applicants, should not be used on any publicly displayed form of identification, and should be transmitted over the Internet only if encrypted. An employer should also

[7] Kate Spooner, "Identity Theft In The Workplace," Privacy Weekly, at 4 [May 28, 2003].

[8] 45 C.F.R. pt. 164, 530 [c] [2003].

[9] Wash. Rev. Code §[19.215.020 [2003].

[10] Cal. Civ. Code §[1798.85 [2003].

[11] S. 745, 108th Cong., 1st Sess., §[§[201-10 [2003].

[12] 649 N.W.2d 859 [Minn. 2003].

consider exploring with its health insurer the use of random numbers, rather than social security numbers, for identifying employee participants.

The data protection/privacy policy also should detail how the employer will control access to, and safeguard, sensitive personal data. To reduce the risk that unauthorized uses and disclosures will go undetected, the policy should explain how employees can identify and report possible security breaches. The policy should also describe how the employer will mitigate potential losses when a security breach does occur.

The employer should regularly audit compliance with the policy, and should also consider requiring employees to sign confidentiality agreements.

Controlling Access to Sensitive Data. Access to sensitive employee data should be restricted, controlled and monitored. The employer should identify the categories of employees who may access sensitive data and the categories of sensitive data that may be used and disclosed by each employee granted access. Access to sensitive data should be limited to employees with a track record for trustworthiness, or who have been subjected to a background check consistent with the Fair Credit Reporting Act.[13]

Upon terminating an employee with authorized access to sensitive data, the employer should promptly change all passwords and security codes available to the terminated employee and require the return of computer disks, compact disks, keys and laptop computers. In addition, the employee's computer should be stripped of sensitive data before being re-issued to another employee.

Temporary, outsourced, and vendor employees should be barred from sensitive data except when absolutely necessary. When access is necessary, the employer should conduct a background check or ensure that the temp agency, outsourcer or vendor has done so, and also insist that such non-regular employees be bonded. The employer should monitor these employees' use and disclosure of sensitive data to the maximum extent feasible.

Technical and Physical Safeguards. The employer's information technology department should put in place an array of security measures for electronic data. All sensitive data should be password protected and, where appropriate, encrypted. Passwords should be changed regularly and varied. Firewalls and anti-virus software need to be installed and regularly updated. Patches for security holes should be promptly implemented.

Maintaining a log of each individual who has accessed files containing sensitive data, creating an audit trail as to where a file has been sent, and monitoring this information can help the employer to promptly detect a security breach. Downloading sensitive data to laptops or to computer or compact disks should be prohibited except with high-level approval from the system administrator. Computers, particularly those used by employees with access to sensitive information, should automatically lockdown if unused for a designated period of time.

Implementing procedures for securing sensitive data in paper format remains essential as well. Paper documents containing sensitive data should be stored only in areas with employees authorized to access those documents. These employees should lock all file drawers, cabinets, and offices containing sensitive paper records when unattended. Computer printers and fax machines for employees who use and disclose sensitive data as part of their job functions should be maintained in a controlled area. The memory dial program on that fax machine should be regularly monitored for outdated and incorrect numbers.

Periodic and proper destruction of sensitive data also is a critical element of any data protection program. Paper files should be shredded internally or by a bonded company. Before discarding or selling any electronic media on which sensitive information is stored, information technology staff or an outside consultant should ensure that no sensitive data can feasibly be retrieved.

Training. Like any workplace policy, a data protection/privacy policy has value only if employees understand it and abide by it. Consequently, central to the policy's success will be a program to train employees -- especially those with access to sensitive data -- to reduce security risks and vulnerabilities, to detect possible security breaches, and to respond to a suspected security breach.

Employees should be required to wear picture identification and to report unfamiliar persons on the premises. The training should encompass "password etiquette," i.e., selecting unpredictable passwords and avoiding disclosure of passwords to co-employees and outsiders. Teaching employees proper procedures for storing, printing, and transmitting documents containing sensitive data also can go a long way to reducing the risk of identity theft. Finally, training employees to recognize and report a suspected security breach will help the employer react quickly to mitigate the potential damage resulting from the breach.

Responsive Remedial Actions

Even when an employer has established and fully implemented a comprehensive data protection/privacy policy, its employees still may be victimized by an identity thief. The data protection policy, therefore, should include a contingency plan to help the employer react appropriately when a security breach is confirmed. Because each security breach has the potential to raise a distinct set of issues, this aspect of the data protection/privacy policy should be phrased in terms of the following general guidelines, rather than as proscriptions:

•Contact Law Enforcement. Identity theft is a federal offense under the Federal Identity Theft and Assumption Deterrence Act,[14] and a felony in most states.[15] However, federal or state law enforcement authorities may be less likely to investigate, or to prosecute, if the employer's information technology personnel have taken steps which arguably taint the evidence of the crime. To avoid

[13] 15 U.S.C. §[1681 [2003].

[14] 18 U.S.C. §[1028 [2003].

[15] See, e.g., NY CLS Penal §[190.79 [2003].

this problem, an employer should consider contacting law enforcement upon first notice of a security breach to discuss whether and how to conduct its own internal investigation so as not to interfere with a criminal inquiry. Reporting the crime also could be important in the event the employer seeks insurance coverage for its losses.

•Notify Employees And Other Potential Victims. California currently is the only state which requires notice to individuals whose personal information was, or is reasonably believed to have been, acquired by an unauthorized person.[16] Promptly notifying victimized employees, nonetheless, is advisable as a matter of courtesy and as a means of mitigating damages. Employees who quickly advise credit bureaus, credit card companies, and banks that their personal information has been compromised are far less likely to suffer significant economic losses. Before notifying employees, the employer should consult with the law enforcement officials assigned to the case to ensure that the notice will not compromise the criminal investigation.

•Help Employees Protect Themselves. Because employees may not know how best to protect themselves from the abuse of their personal information, the employer should consider a response plan. Depending on the nature and magnitude of the data loss, such a plan might include designating a human resources representative to answer questions and provide assistance, and/or preparing a form letter to the three major credit bureaus [Equifax, Experian and Transunion] placing a security alert on the employee's account and requesting a free credit report to permit the employee to check for bogus credit activity.

The employer also should make the affected employee aware of other available resources to assist in combating identity theft. The FTC, for example, distributes free copies of its excellent publication, "Identity Theft: When Bad Things Happen To Your Good Name"; maintains a toll-free number for the FTC Identity Theft Data Clearinghouse [1-877-IDTHEFT]; and operates a useful Web site [www.consumer.gov/idtheft]. Beginning May 1, 2004, the Financial Services Roundtable, an organization representing 100 financial institutions which handle approximately 70 percent of the economy's financial transactions, will sponsor a program -- known as the Identity Theft Assistance Center -- to permit those who believe they have been victimized by identity theft to notify all potentially affected credit card companies and financial institutions as well as law enforcement with one phone call to their local bank.[17]

Legislation adopted by Congress shortly before this article went to press and expected to be signed by President Bush would significantly supplement these resources. If enacted, the new law would require the major credit bureaus to provide each consumer with a free credit report annually upon request, to permit consumers to place a security alert on their credit reports, and to enable consumers to inform one credit bureau of the possible identity theft and have that information shared with all.[18]

Employees whose personal information already has been used to make fraudulent charges or to open fraudulent accounts should be advised to request that the security departments of affected creditors and financial institutions promptly close these accounts in addition to taking the steps listed above.

Conclusion

As the repositories of vast quantities of personal data, employers are prime targets for identity thieves. No employer wants to be the unsuccessful "test case" in a class action lawsuit by employees whose personal data was stolen, alleging that the employer's negligence resulted in their being victimized by identity thieves. To avoid that fate, employers should implement a comprehensive data protection/privacy policy and prepare a contingency plan in the event that they and their employees, nonetheless, fall victim to America's fastest-growing crime.

[16] See, Cal. Civ. Code §[1798.82 [2003].

[17] New Identity Theft Alert System Tested, posted at www.cnn.com [last visited Nov. 24, 2003].

[18] H.R. 2622, 108th Cong. 1st Sess. §[501 [2003].