Identity Theft

Protecting Your Employer-Client from Liability

by Todd Presnell

The phrase "identity theft" is unfortunately now commonplace in America's lexicon. The phrase generally refers to the act of stealing another's personal financial information and using that information to fraudulently purchase, use, and/or convert merchandise or services. The act of identity theft takes many forms, and these fraudulent acts are occurring increasingly either at an employer's workplace or through the use of information, such as social security numbers and bank account numbers, that an employer stores concerning its employees.

With the increase in identity theft in general, and identity theft at the workplace in particular, victims of identity theft are looking for restitution, and other damages, from the companies from which the information was stolen. This article, therefore, examines the recent increase in identity theft, including the variety of forms that it takes and the methods by which information is stolen from employers. It also provides an overview of the laws pertaining to identity theft and discusses the theories of employer liability arising out of the inadvertent release of the personal, financial information about employees. Finally, the article offers practical tips for employers and their attorneys regarding how to prevent identity theft in the workplace and avoid liability.

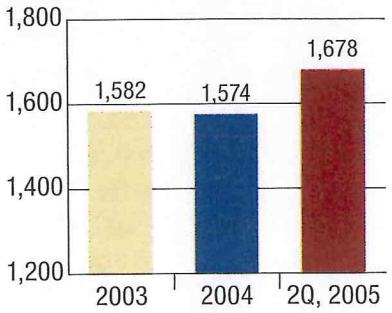
Identity Theft Is on the Rise

There is no question that incidents of identity theft are rising exponentially. The Federal Trade Commission (FTC) sponsored a survey, completed in May 2003, "of U.S. adults on the topic of identity theft and the resulting experiences of victims." Federal Trade Commission, *Identity Theft Survey Report*, Sept. 2003, available at http://www.consumer.gov/idtheft/pdf/synovate_report.pdf. Using these survey results, the FTC concluded that 9.91 million Americans had discovered that they had been victimized by identity theft within the prior year. *Id.* at p. 4, 7, and Table 2. The method of such identity thefts included use of lost or stolen credit cards, but also the theft of social security numbers and other personal information that was "misused by someone who had access to it such as a family member or a workplace associate." *Id.* at p. 30–31.

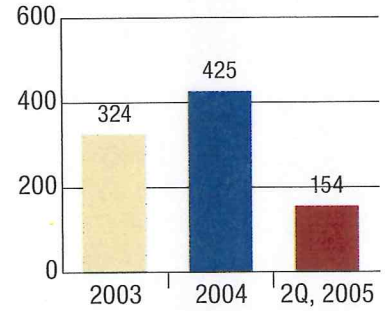
The number of identity theft complaints filed with the FTC has increased dramatically, rising to 162,000 in 2002 and to 246,000 in 2004. Federal Trade Commission, *National and State Trends in Fraud and Identity Theft*, Feb. 1, 2005, http://www.consumer.gov/. The Federal Bureau of Investigation, moreover, describes identity theft as "pervasive and growing" and states that it "has emerged as one of the dominant white collar crime problems of the 21st Century." *Financial Crimes Report to the Public*, U.S. Department of Justice, Federal Bureau of Investigation, May 2005, available at http://www.fbi.gov/publications/financial/fcs_report052005/fcs_report052005.htm. In fact, the number of identity theft investigations pending with the FBI at the close of FY2004 totaled 1,574. Through the second quarter of FY2005, however, that number had increased to 1,678. Similarly, the number of identity theft indictments totaled 482 for FY2004, and was at 230 by the end of the second quarter of FY2005. These numbers are illustrated in the charts above, right. *Id.*

In short, it is clear that consumer complaints about, and governmental investigations of, identity theft are increasing at a rapid rate. It should be equally clear, therefore, that the incidents of identity theft in the workplace are rising and will continue to rise proportionally.

Identity Theft Pending Cases



Identity Theft Convictions/ Pretrial Diversions



Methods of Identity Theft

In general terms, identity theft is the misappropriation and fraudulent use of a person's personal or confidential information. Such information includes, for example, social security numbers, drivers' license numbers, names, addresses, dates of birth, credit card numbers, PINs, and bank account numbers. Federal and state laws imposing criminal penalties for identity theft may define identity theft differently. For instance, the federal Identity Theft and Assumption Deterrence Act of 1998 defines the crime of identity theft as the use of "a means of identification of another person" coupled with the intent to use the information fraudulently. 18 U.S.C. §1028. However defined, this is, of course, exactly the type of information contained in a company's personnel files on its employees, which makes such records, whether maintained in a file folder or electronically, a ripe resource for identity thieves.

The methods of identity theft from information maintained by employers is limited only by the bounds of imagination of a technologically savvy criminal. These methods include sophisticated computer hacking strategies that have made news headlines over the last couple of years. For instance, at Boston College, a computer program con-

Todd Presnell is a member of Miller & Martin PLLC, a full service law firm with offices in Nashville, Atlanta and Chattanooga. **This article was prepared in conjunction with DRI's Employment Law Teleconference seminar, and Mr. Presnell acknowledges the contributions to this article by the presenters at that seminar, Lawrence Sommerfeld of the U.S. Attorney's Office in Atlanta, and Cynthia A. Bremer of Flynn, Gaskins & Bennett, LLP in Minneapolis.**

taining the names and social security numbers of up to 120,000 BC alumni was accessed by hackers in March 2005. *See* http://www.msnbc.msn.com/id/7221456, Mar. 17, 2005. In April 2005, LexisNexis disclosed that confidential information such as social security numbers and driver's license numbers may have been stolen from its database via unauthorized access. *See* http://abcnews.go.com/Business/wireStory?id=666708, Apr. 13, 2005. In June 2005, MasterCard and Visa revealed that the computer network of its third-party processor, CardSytems Solutions, Inc., was hacked, giving access to the credit card numbers of over 40 million card holders. *See* http://www.washingtonpost.com/wp-dyn/content/article/2005/06/17/AR2005061701031.html, June 18, 2005.

Yet, reports suggest that the overwhelming majority of identity theft incidents in the workplace occur through simpler, unsophisticated means such as the copying of personnel files from an unlocked file room or through an employee's downloading confidential information from a company's network. Many times the access to an employee's confidential information is the result of thoughtless yet inadvertent actions of employers. For example, lawsuits have arisen where a company faxed a list of employees' names and social security numbers to 16 different managers, *Bodah v. Lakeville Motor Express, Inc.*, 663 N.W.2d 550 (Minn. 2003), where a union permitted its treasurer to take home a list of employees containing their confidential information, *Bell v. Michigan Council 25 of the American Federation of State, County, and Municipal Employees, AFL-CIO, Local 1023*, 2005 WL 356306 (Mich. Ct. App. Feb. 15, 2005), and where a box of personnel records was kept in a storage area. *See* Employment Records Prove Ripe Source for Identity Theft, *USA Today*, Jan. 23, 2003, available at http://www.usatoday.com/money/workplace/2003-01-23-idtheft-cover_x.htm. These examples show that, while identity theft in the workplace can be the result of complex computer hacking strategies, identity thieves need little sophistication to accomplish the same tasks.

Relevant Laws and Theories of Liability

Statutory

Some statutory law exists that, at least in some way, addresses the pervasive identity theft problem. For example, the Electronic Fund Transfer Act, 15 U.S.C. §1693 *et seq.*, offers protections for persons using electronic means, such as a debit card, to debit or credit an account. The Fair Credit Reporting Act, 15 U.S.C. §1681 *et seq.*, requires, among other things, that a person's credit record only be provided for legitimate business needs. The Health Insurance Portability and Accountability Act of 1996 (HIPAA) also requires employers to protect confidential medical records which, of course, may contain an employee's identifying information. 29 U.S.C. §1181 *et seq.* In 1998, Congress passed the Identity Theft and Assumption Deterrence Act, 18 U.S.C. §1028(a)(7), which criminalizes actions by a person who:

> Knowingly transfers or uses, without lawful authority, a means of identification on another person with the intent to commit, or to aid or abet, any unlawful activity that constitutes a violation of Federal law, or that constitutes a felony under any applicable State or local law.

Identity theft is limited only by the bounds of imagination of a technologically savvy criminal.

This act, however, is purely criminal in nature, and does not provide a private right of action to victims of identity theft crimes. *See, e.g., Garay v. U.S. Bancorp*, 303 F. Supp. 2d 299 (E.D.N.Y. 2004); *Booth v. Equifax Credit Information Services, Inc.*, 2001 WL 34736212 (D. Or. 2001). *See generally* William E. Harsfield, Investigating Employee Conduct, §12:19 (Supp. Nov. 2005).

These acts address tangentially the identity theft problem in the workplace. In December 2003, however, Congress passed the Fair and Accurate Credit Transactions Act (FACTA), which is an amendment to the Fair Credit Reporting Act. 15 U.S.C §1681w. Specifically, this Act requires that any person who "maintains or otherwise possesses consumer information, or any compilation of consumer information, derived from consumer reports for a business purpose to properly dispose of any such information or compilation." 15 U.S.C. §1681w(a)(1). FACTA "is designed to reduce the risk of consumer fraud and related harms, including identity theft, created by the improper disposal of consumer information." 16 C.F.R.682.2(a). The term "consumer information" "means any record about an individual, whether in paper, electronic, or other form, that is a consumer report or is derived from a consumer report." 16 C.F.R.682.1(b).

FACTA, therefore, specifically requires an employer to take reasonable measures in disposing of an employee's credit report obtained as part of the employer's hiring process. In fact, the Fair Credit Reporting Act defines "consumer report" so as to include background checks on applicants for employment or other information, such as medical history, residential history, or check-writing history, gained by the employer regarding its employees. 15 U.S.C. §1681a(d). FACTA does not require employers to destroy records containing an employee's confidential information, such as background reports, or ignore policies and laws regarding mandating retention of such documents. *See* 15 U.S.C. §1681w(b); 16 C.F.R. §682.4. Rather, FACTA requires that employers take reasonable measures when they dispose of personal, consumer information that they obtain on employees or prospective employees. *See generally* Paul J. McCue, *Preventing Identity Theft: Must Employers Shred Background Reports*, 34 Colo. Lawy. 101 (Nov. 2005).

The FTC, moreover, has issued regulations setting a threshold for what employers must do to "properly dispose" of a person's (read: employee's) consumer information. First, the FTC de-

fines "disposal" or "disposing" as "[t]he discarding or abandonment of consumer information," or "[t]he sale, donation, or transfer of any medium, including computer equipment, upon which information is stored." 16 C.F.R. 682.1(c)(1) & (2). Second, the FTC pronounced a "standard" for complying with the disposal requirements:

> Any person who maintains or otherwise possesses consumer information for a business purpose must properly dispose of such information by taking reasonable measures to protect against unauthorized access to or use of the information in connection with its disposal.

16 C.F.R. 682.3(a). The FTC went on to provide "examples" of what it meant by "reasonable measures," which included the following:

- Implementing policies and procedures that require the "burning, pulverizing, or shredding" of documents containing consumer information "so that the information cannot practicably be read or reconstructed";
- Implementing policies and procedures for erasing electronic media that contains consumer information;
- Monitoring compliance with these policies and procedures; and
- Entering into a contract, "[a]fter due diligence," with a third party to properly destroy documents and electronic media containing consumer information, and monitoring the third party's compliance with the contract, including securing an independent audit of the third party.

16 C.F.R. 682.3(b)(1)–(3).

In addition to this relatively new federal statute, many states have enacted their own versions of identity theft laws. For example, California passed a law requiring companies to notify California residents when their personal information has been accessed. Cal. Civ. Code §1798.29. Michigan recently passed a law requiring companies that obtain social security numbers in the regular course of business to maintain a written policy that requires the numbers to be kept confidential, limits access to such information, mandates procedures for disposal, and enacts penalties for violation of these policies. Mich. Comp. Laws Ann. §445.84. Many other states have either passed or proposed similar legislation. For up-to-date information on the status of these laws or bills, as well as new legislation in other states, see the website of the National Conference of State Legislatures, http://www.ncsl.org.

Common Law

Predictably, employees are thinking creatively about potential causes of action or theories of recovery for damages incurred when their personal, confidential information is stolen from their workplace. Although the case law in the identity theft area is in the embryonic stages, at least two theories have emerged as legitimate avenues of relief—the tort of invasion of privacy and general negligence. The leading case in each of these areas is discussed below.

Invasion of Privacy

Relevant to our discussion here, the Restatement outlines the tort of invasion of privacy as follows:

> One who gives publicity to a matter concerning the private life of another is subject to liability to the other for invasion of his privacy, if the matter publicized is of a kind that
> (a) would be highly offensive to a reasonable person, and
> (b) is not of legitimate concern to the public.

Restatement (Second) of Torts §652D. The Restatement further explains that the term "publicity" is a key component of the tort, meaning a situation where "the matter is made public, by communicating it to the public at large, or to so many persons that the matter must be regarded as substantially certain to become one of public knowledge." *Id.*, Cmt. a. The Restatement further explains that liability only attaches when the publicity concerns "the private, as distinguished from the public, life of the individual." *Id.*, Cmt. b. As examples, the Restatement presumes that a person's date of birth is a matter of public record, the publicity of which will not impose liability, while a person's tax return is a private matter the publicity of which should constitute an invasion of privacy. *Id.*

Against this backdrop, the Supreme Court of Minnesota had the opportunity to explore the application of the tort of invasion of privacy to a company's unauthorized release of personal, confidential information about its employees. In *Bodah v. Lakeville Motor Express, Inc.*, 663 N.W.2d 550 (Minn. 2003), a Minnesota-based trucking company, Lakeville Motor Express (LME), through its Safety Director, "sent a facsimile transmission to the terminal managers of 16 freight terminals" for the purpose of "allow[ing] LME to keep computer records for terminal accidents-injuries, etc." *Id.* at 552. The fax transmission included a five-page list containing the names and social security numbers of 204 LME employees. *Id.*

The employees complained to their union representative, and the head Union Steward confronted LME officials about the dissemination of the employees' social security numbers. A few months later, the president of LME sent a letter to LME employees notifying them of the dissemination and telling them that all terminal managers had been instructed "to destroy or return the list immediately." It also appeared that the managers heeded this instruction, and the list of employees was not disseminated further. *Id.* at 552–53.

Shortly thereafter, the employees filed a class action "alleging that LME's dissemination of their social security numbers to the 16 terminal managers constituted an invasion of their right to privacy." *Id.* at 553. Upon consideration of a Rule 12 motion, the trial court dismissed the complaint on the grounds that the "dissemination did not constitute 'publicity' under a claim for publication of private facts." *Id.*

The Minnesota Court of Appeals reversed the trial court's decision, stating that "[a]n actionable situation requires a level of publication that unreasonably exposes the [employee] to significant

risk of loss under all the circumstances." *Bodah v. Lakeville Motor Express, Inc.*, 649 N.W.2d 859, 866 (Minn. Ct. App. 2002). In so ruling, the court of appeals was receptive to the potential damage that could occur to an employee if his or her social security number fell into the wrong hands. Specifically, the court stated that social security numbers are "such a significant identifier that they facilitate access by others to many of our most personal and private records and can enable someone to impersonate us to our embarrassment or financial loss," and recognized that "[t]his is part of the so-called identity-theft phenomenon that is an increasing risk and problem in our society." *Id.* at 862–63.

The Minnesota Supreme Court, however, reversed the court of appeals and reinstated the trial court's decision to dismiss the case. The supreme court rejected the court of appeals' publicity standard and opted to adhere to the definition of the Restatement. 663 N.W.2d at 558–59. Under the Restatement standard, moreover, the court found that the "disseminat[ion] [of] 204 employees' social security numbers to 16 terminal managers in six states does not constitute publication to the public or to so large a number of persons that the matter must be regarded as substantially certain to become public." *Id.* at 557–58.

Although the plaintiffs' complaint ultimately did not survive a Rule 12 motion, the *Bodah* case certainly does not foreclose the real possibility that an employer's failure to control dissemination, or to permit unauthorized access to, social security numbers and other employee identifying information will lead to civil lawsuits based upon the tort of invasion of privacy. The court of appeals clearly recognized the potential damage to employees when their personal, confidential information is accessed by unauthorized persons. Moreover, while the supreme court found that dissemination of personal information to 16 managers within the company did not constitute the requisite publicity, surely the release of such information to the public at large—as opposed to internal managers—would meet the publicity requirement of the Restatement. In short, the LME employees' attempt to state a cause of action for invasion of privacy failed in *Bodah*, but this tort remains a strong avenue of relief for employees when their identities are stolen by third parties from the workplace.

Negligence

The *Bodah* court also offered the opinion, via *dicta* contained in a footnote, that, "if an unauthorized transmission of private data actually resulted in pecuniary loss due to identity theft, a plaintiff may be able to bring a negligence action." *Id.* at 556 n.5. The court went on to say that, "[l]ikewise, a plaintiff may have a cause of action for negligent infliction of emotional distress if, because private information was shared, the plaintiff suffered severe emotional distress with accompanying physical manifestations." *Id.*

The foreseeability argument regarding identity theft is difficult to counter.

Only a few months before the *Bodah* court made these statements, a jury in Michigan rendered a sizeable verdict against a union under these same theories. Specifically, in *Bell v. Michigan Council 25 of the American Federation of State, County, and Municipal Employees, AFL-CIO, Local 123*, 2005 WL 356306 (Mich. Ct. App. 2005), *appeal denied*, 707 N.W.2d 597 (Mich. Dec. 28, 2005), the plaintiffs, emergency service operators (911 operators) for the City of Detroit, were members of the AFSCME Union. For union membership purposes, the city obtained certain personal information on these employees and, in turn, provided the union with a quarterly report of all personnel, including the plaintiffs, who were members of the union. This report "contained each employee's job classification, social security number, and pension number." *Id.* at *1. The union, in turn, provided this report to its treasurer so that she could compare it with a similar report generated by the union to ensure accuracy of the union membership.

The local authorities later arrested the treasurer's daughter after it was discovered that she had somehow obtained the 911 operators' names, social security numbers, and drivers' license numbers. *Id.* The daughter subsequently pleaded guilty of participating in a scheme to use this confidential information to purchase illegal phone services and other goods.

This episode was a classic example of identity theft from the workplace. The 911 operators, therefore, sued the union on a simple negligence theory, alleging that it "was liable for not safeguarding their personnel information and that this negligence facilitated the identity theft perpetrated by" the treasurer's daughter and her cohorts. *Id.* The union moved in succession for summary judgment, directed verdict, and for JNOV, all of which were denied by the trial court. The jury found the union liable under a negligence theory and returned a verdict in favor of the plaintiffs for $275,000. *Id.*

Building upon the loss of its dispositive motions, the union appealed the case, arguing primarily that it had no duty—the first prong of any negligence action—to the plaintiffs for the "unforeseeable criminal acts of a third party." *Id.* at *2. The appellate court, therefore, examined the elements necessary to impose a duty upon a party to protect against the acts of third persons. The court noted that there is no such duty "absent a special relationship between the defendant and the plaintiff or the defendant and the third party." *Id.* Whether such a "special relationship exists between the defendant and the plaintiff requires considerations of, among others, the societal interests involved, the severity of the risk, the likelihood of the occurrence of the risk, the relationship between the parties, and the foreseeability of the harm. Here, the union challenged the imposition of a duty by arguing that the risk

Identity Theft, continued on page 78

Identity Theft, from page 12
of the criminal act (identity theft) was not reasonable or severe, and that the likelihood of its occurrence was not foreseeable because "criminal activity by its very nature is unforeseeable." *Id.*

The appellate court swiftly rejected these arguments. As a preliminary part of the analysis, the court noted the fiduciary-like duty that exists between a union and a union member. The court stated that "[i]t follows that part and parcel of that relationship is a responsibility to safeguard its members' private information" and, furthermore, "society has a right to expect that personal information divulged in confidence... will be guarded with utmost care." *Id.* at *3.

Regarding the foreseeability issue, the court agreed that the focus is not upon the third party's particular actions, *i.e.*, the method of the theft, but rather "the foreseeability of the harm, identity theft." *Id.* at *4. Regarding the foreseeability of identity theft, the court had this to say:

> The crime of identity theft has been gaining momentum in recent years due to the accessibility of identifying information, mainly through computer use. In the past, the risk of harm stemming from a worker taking home sensitive information may not have been great. However, with the advancements in technology, holders of such information have had to become increasingly vigilant in protecting such information and the security measures enacted to ensure such protection have become increasingly more complex.... [T]he severity of the risk of harm in allowing personal identifying information to be taken to an unsecured environment is high. The instant plaintiffs were very fortunate regarding the limited extent of the fraud perpetrated using their identities. But it is the potential severity of the risk, not the actual risk encountered, that must be considered in deciding to impose liability.

Id.

The court found, therefore, that a special relationship existed between the union and its members, such that the union owed them "a duty to protect them from identity theft by providing some safeguards to ensure the security of their most essential confidential identifying information, information which could be easily used to appropriate a person's identity." *Id.* at *5. Thus, the $275,000 jury verdict was upheld.

To be sure, the *Bell* court limited its holding to the facts of the case—where the defendant "knew confidential information was leaving its premises and no procedures were in place to ensure the security of the information." *Id.* Nevertheless, the court's analysis of the special relationship between the union and union member is equally persuasive when the relationship is employer and employee. Moreover, the foreseeability argument regarding identity theft is difficult to counter. These salient points, coupled with the ever-increasing state laws imposing express duties on employers to protect their employees' confidential information, will no doubt form the basis of negligence actions by employees against employers when their confidential information is accessed by third parties.

Methods of Prevention and Avoidance of Employer Liability

With the enactment of federal and state laws regarding the protection of information from identity theft, the certainty of additional bills being introduced in state legislatures, and the common law causes of action—invasion of privacy and negligence—providing employees with private causes of action, it is imperative that employers become proactive in guarding against identity theft in the workplace. Outlined below, therefore, are general tips for complying with these duties, which should serve the added goal of avoiding or limiting liability in the event identity theft nevertheless strikes the workplace.

- Establish a policy prohibiting the dissemination of employees' personnel files or other files that may contain confidential information such as social security numbers, drivers' license numbers, etc.
- Establish a policy outlining the types of confidential information that actually are needed during the hiring process, and expressly forbidding the collection of confidential information that is not really necessary.
- Establish a separate confidential policy that limits employees' access to confidential information.
- Establish a policy for the prompt and proper disposal of confidential information that is no longer needed, specifically including information gained from "consumer reports."
- Maintain separate filing system/location for documents containing confidential information.
- Implement appropriate software to protect against computer viruses, unauthorized access to a company's computer network, and similar online or electronic invasions of electronic data storage systems.
- Establish a policy that requires regular and periodic monitoring of the policies listed above to ensure that they are working, including regular testing and auditing of such policies.
- Implement a regular training program for appropriate employees (if not all of them) on the importance of proper handling of confidential information.
- Establish a mandatory reporting system whereby employees must report immediately when they believe their confidential information has been inappropriately accessed, and when they suspect co-workers of engaging in identity theft in general, or unauthorized access to confidential information.

The implementation of these and similar policies and procedures, of course, will not prevent any and all lawsuits, and certainly do not constitute a guarantee against identify theft. They should, however, go a long way in preventing identity theft and limiting or ultimately eliminating an employer's liability when the virtually inevitable identity theft occurs. FD

English, Welsh, from page 76
accident either did not happen as alleged, or that the symptoms are less severe than claimed. Employment records and history invariably assist in quantifying cases but access to these can prove problematic.

Currently, defendants in road traffic accident claims must reimburse the National Health Service for the costs of medical treatment received by claimants as a result of the accident, currently capped at £35,500. In October 2006, a new bill will go before Parliament, which may require defendants to repay NHS charges in all types of personal injury claims. As such it is increasingly important that causation is rigorously investigated. FD