Identify Theft: An Organization's Responsibilities

by

Gregory J. Gerard
Assistant Professor
Department of Accounting
Florida State University
Tallahassee, FL 32306

William Hillison
Andersen Professor of Accounting
College of Business
Florida State University
Tallahassee, FL 32306
850-644-7872
E-mail: bhillis@cob.fsu.edu

Carl Pacini
Associate Professor
Department of Accounting and Finance
Florida Gulf Coast University
10501 FGCU Blvd. S.
Fort Myers, FL 33965-6565

January 2004

Introduction

In this article, we discuss an organization's responsibilities to mitigate the opportunity for identity theft.[1] Identity theft is the criminal act of assuming the identity of another person with the expectation of gain. The gain is normally financial as a result of improperly extending credit, allowing banking transactions, establishing cellular telephone or other utility service, or gaining governmental benefits.

Identity theft will result in the loss of $221 billion worldwide by the end of 2003, with $73.8 billion lost in the U.S. alone. That number equals the total losses from 2002, when identity theft caused more than $73 billion in losses worldwide, with the U.S. accounting for about a third of that with over $24 billion. By 2005, losses from identity theft could amount to $2 trillion worldwide, if the 300 percent compound annual growth rate continues.[2]

Much that has been written on identity theft discusses steps that individuals can take to minimize the risk of theft of their identities. Most of these steps involve protecting the information that individuals have in their possession. Other written material provides advice on what to do if a person is a victim of identity theft. Information is provided about who to contact and how to proceed to alleviate the problems associated with the theft of a person's identity.

In contrast, we address issues related to organizations that collect, assemble, process, store and retrieve information about individuals. We identify the issues, risks, and controls associated with personal information about an organization's customers and other stakeholders. Many organizations may not recognize the potential liability of not controlling information risks. We not only identify this liability risk, but we help those charged with responsibility within an organization to manage and control those risks.

The Extent of the Identity Theft Problem

Identity theft is fast becoming the most pervasive financial crime today. According to the Federal Trade Commission (FTC), identity theft accounted for more than 160,000 complaints in 2002 and was the number one source of consumer complaints for the third consecutive year. Identity theft accounted for over 130,000 or 62 percent of complaints received by the FTC through the first seven months of 2003.[3]

A recent FTC telephone survey involving a sample of more than 4,000 individuals indicated that as many as 27 million Americans were victims of identity theft in the last five years. In the past year, almost 10 million (or 3.4 percent of the population) people were victimized to the tune of $53 billion. The average loss to businesses was $4800 per incident, including $10,200 for new account fraud and $2,100 for card misuse.[4] The average loss for individuals was $500.[5]

The biggest losses resulted from thieves using a victim's personal information to open new accounts. Fraudulent new account openings accounted for $32.9 billion in losses to businesses and $3.8 billion to consumers.[6] In addition to out-of-pocket losses, there is the cost of fighting the problems associated with identity theft. Law enforcement agencies spend about $15,000 on each case and each victim spends about 175 man-hours on dealing with the paperwork restoring order to their financial lives.[7]

Since liability of identity theft victims is limited by law, credit reporting agencies typically have placed the burden of proof on the victim to show debts incurred by identity thieves were not authorized.[8] Creditors and collectors, being well familiar with elaborate disavowals from debtors, generally continue collection efforts in spite of the victim's claims. Ultimately, the unpaid fraudulent accounts are charged-off, leaving the victim abused by collection efforts and financially ruined by adverse credit reports.[9]

In addition to the hassle to victims of clearing up fraudulent bank accounts and credit card debts, the public is put at risk because identity theft is linked to drug trafficking, money laundering, and terrorism.[10] Terrorists have utilized identity theft to obtain employment and access to secure locations such as airports. As Dennis Lormel, Chief of the FBI's Financial Crimes Section, told the House Committee on Financial Affairs in October 2001, "[t]errorist cells often resort to traditional fraud schemes to fund the terrorists' activities. The ease with which these individuals can obtain false identification or assume the identity of someone else, and then open bank accounts and obtain credit cards, make these attractive ways to generate funds." [11]

How Does Identity Theft Occur?

Victims of identity theft often do not realize they have become victims until they apply for financing, review their accounts or receive an alert from a financial institution. In the FTC survey noted above, 52 percent discovered identity theft by monitoring their accounts, 26 percent were alerted by credit card issuers or banks, and 8 percent found out when they were turned down for credit. In addition, victims know even less concerning how the identity thieves secured their personal information. The same FTC survey notes that only half the victims knew how thieves obtained their personal data.[12]

Identity theft occurs in many ways, ranging from careless sharing of personal information, to intentional theft of purses, wallets, mail or digital information, and dumpster diving. Identity theft can be accomplished through simple, low-tech methods such as:

- thieves go through mailboxes in search of pre-approved credit offers or outgoing mail containing checks;
- thieves go through consumer trashcans to find a bank statement, bill payment record or other document containing personal information;
- thieves engage in "shoulder surfing"—watching a person from a nearby location as he or she enters a credit card number, ATM PIN, or calling card number;
- con artists phone people at home or work and try to fool them into revealing personal information over the phone. They may pose as representatives of a charity, utility, or bank;

- fraudsters engage in "pretexting"—they contact a credit bureau or financial institution and falsely claim to be another person having a right to access identity information; and
- fraudsters engage in "dumpster diving" outside businesses or medical facilities to obtain personal information on customers.[13]

Identity theft can also be perpetrated using high-tech methods. Here are some examples:

- computer criminals evade security walls to hack into corporate databases and steal personal information;
- con artists send unsolicited emails with fake offers or scams that evoke sympathy. These offers entice victims to respond with information that includes personal data;
- fraudsters bribe employees at businesses that maintain centralized data centers gaining illegal access to thousands of personal consumer records;
- fraud rings tamper with non-bank ATMs to steal bank account data of ATM users;
- restaurant waiters and retail clerks swipe their customers' credit or debit cards through an illegal, hand-held device that copies information from the magnetic strip on the card's back; and
- thieves use software that mirrors keystrokes on a computer or website.[14]

Knowledge of identity theft techniques is important but it is only a first step. Both Individuals and organizations must be proactive in reducing the opportunities for the commission of identity theft. Although most organizations cannot directly influence the actions of identity thieves, they can implement procedures and programs that can reduce the likelihood of or opportunities for identity theft. Many organizations or entities, however, do not take the appropriate steps to curb opportunities for identity thieves. In a 2003 survey conducted by Harris Interactive Service Bureau and compiled by Vontu, a provider of software security solutions, the following key findings were noted:

- 62 percent of survey respondents reported that incidents at work could put customer data at risk for identity theft;
- 66 percent said their co-workers, not hackers, pose the greatest risk to consumer privacy;
- 70 percent said that government regulations play a role in raising awareness at their workplace about identity theft and database security;
- Nearly 50 percent said that government still has not done enough to help thwart identity theft;
- 46 percent said it would be "easy" to "extremely easy" for workers to remove sensitive data from a corporate database; and

32 percent were unaware of internal company policies to protect confidential customer data.[15]

Two related Oregon cases illustrate many of the factors noted above.[16] A ring of identity thieves obtained personal information by stealing mail, garbage, and recycling material and by hacking into websites and personal computers. The thieves exchanged the stolen information for methamphetamines, cellular phones or other favors. Before arrest, the thieves had gained access to about 400 credit card accounts and made about $400,000 in purchases on fraudulently obtained credit card accounts. One scheme involved the theft of pre-approved credit card solicitations, activating the cards, and having them sent to drop boxes or third-party addresses. Another scam involved collecting names, dates of birth, and social security numbers from discarded medical, insurance, or tax information and obtaining credit cards over the Internet. Another artifice used by the fraudsters entailed software to hack into commercial websites or personal computers and mirror keystrokes to capture credit card data.[17]

What Laws Apply to Identity Theft?

Federal laws applicable to identity theft may be used for prosecution of identity theft offenses and/or to assist victims in repairing their credit history. On October 30, 1998, Congress passed the Identity Theft and Assumption Deterrence Act (ITADA).[18] The law defines identity theft as any act committed by one who "[k]nowingly transfers or uses, without lawful authority, a means of identification of 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." [19] The statute is limited to the use of the "[m]eans of identification of another person."

The statute defines "means of identification" to include "any name or number that may be used, alone or in conjunction with any other information, to identify a specific individual."[20] Specific examples covered by this statutory language are: name, social

security number, date of birth, driver's license and other numbers, fingerprints, voiceprint, retina or iris image, or other biometric identifiers, any unique telecommunication identifying information, or access device.[21]

ITADA contains stiff criminal penalties for its violation. The law provides for imprisonment of not more than 15 years when a person commits an offense that involves the transfer or use of one or more means of identification if, as a result of the offense, anything of value greater than one thousand dollars during any one-year period is obtained.[22] Otherwise, the statute provides for imprisonment of not more than three years. ITADA also contains a provision that provides for the forfeiture of any personal property used or intended to be used to commit the offense. Otherwise, the statute provides for imprisonment of not more than three years. ITADA also contains a provision that provides for the forfeiture of any personal property used or intended to be used to commit the offense.

ITADA also requires the FTC to establish procedures to handle complaints from victims of identity theft and to provide educational materials to these victims. The FTC has created a website and set up a hotline for victims.[23]

Numerous cases have been prosecuted under ITADA. Recently, in *U.S. v. Davis*,[24] the Sixth Circuit Court of Appeals upheld a conviction of a man who was the leader of a conspiracy to acquire, use and sell fraudulent credit information. The defendant had access to databases (through his employment) containing credit records, social security numbers, addresses, and employment histories, from which he would obtain the identities of individuals with good or no credit history and the sell those identities to persons with the same or similar names. In another case, *U.S. v. Jackson,*[25] the Second Circuit upheld the guilty plea of a man on charges of identity theft. The defendant began by identifying a wealthy target, usually an executive, by searching the Internet. He would purchase personal information about the executive from an

"information broker" on the Internet, place calls to banks, credit card companies and then use the originally acquired personal data to convince whomever he was speaking to that he was the executive. He would thereby acquire account numbers, expiration dates, etc. and change the billing address to a hotel. The defendant would order merchandise, such as diamonds, and have courier services or hotel employees take delivery. He would later pose as the executive and sell the delivered goods for cash. The defendant was sentenced to eight years in prison.

Another federal law relevant to identity theft is the Fraudulent Access to Financial Information (FAFI) section of the Gramm-Leach-Bliley Act (GLB).[26] The statute forbids the acquisition of financial institution customer data by means of false pretenses. The law also directs banking regulators to ensure that financial institutions have policies, procedures, and controls to prevent unauthorized disclosures of customer information.[27] In May, 2002, the FTC released a "Safeguards Rule" which requires financial institutions to develop, implement, and maintain a comprehensive information security program (ISP) to protect customer information.[28] Each financial institution under FTC jurisdiction must have implemented an ISP no later than May 23, 2003.

Five basic elements factor into development and implementation, as well as risk assessment, management, and control, of an ISP. Each financial institution shall:

- designate an employee or employees to coordinate the ISP;
- identify reasonably foreseeable internal and external risks to the security, confidentiality and integrity of customer information that could result in the unauthorized disclosure, misuse, alteration, destruction, or other compromise of such information, and assess the sufficiency of any safeguards in place to control the risks;
- design and implement information safeguards to control the risks identified through risk assessment, and regularly test or otherwise monitor the effectiveness of the safeguards' key controls, systems, and procedures;
- oversee service providers (financial institution vendors who have access to customer information) by: (i) taking reasonable steps to select and retain service providers that are capable of maintaining safeguards for customer information; and (ii) requiring service providers by contract to implement and maintain such safeguards; and

- evaluate and adjust the ISP in light of the results of the required testing and monitoring, any material changes to operations or business agreements, or any other circumstances that a financial institution knows or has reason to know may have a material impact on the ISP.[29]

Violators of FAFI are subject to a criminal penalty of imprisonment of not more than five years and a fine of not more than $250,000 for individuals or $500,000 for organizations.

Although the issue remains unsettled, a failure to comply with the Safeguards Rule is a violation of federal law subject to FTC enforcement and potentially giving rise to individual or class action claims under a state unfair and deceptive trade practices law or even a contract theory.[30] Financial institutions should also be cognizant of their potential for being held accountable if their vendors are not meeting the safeguard requirements as to customer information.[31]

A third federal law that creates liability for identity thieves and various third parties is the Health Insurance Portability and Accountability Act (HIPAA).[32] The law includes a criminal statute that involves vast legal risk for health care providers and other members of the health care industry.[33] A person who knowingly commits any of a series of acts violates federal law. These violations involve one who:

1. uses or causes to be used a unique health identifier;
2. obtains individually identifiable health information relating to an individual; or
3. discloses individually identifiable health information to another person.[34]

"Individually identifiable health information" means any information, including demographic information, collected from a person that is created or received by a healthcare provider, health plan, employer, or healthcare clearinghouse, that relates to the past, present, or future health of a person and identifies that individual (or gives a reasonable basis to believe that the information can be used to identify the person).[35]

One who violates that HIPAA statute may be fined not more than $50,000 nor imprisoned for more than one year or both. If the offense is committed with the intent to

use personal information for economic gain (e.g., identity theft) then the fine can rise to $250,000 and imprisonment can increase to 10 years.[36]

A fourth federal law that is pertinent to identity theft is the Fair Credit Reporting Act.[37] The law establishes standards for gathering and reporting both credit and character-based information. It also sets forth procedures and timeframes for correcting mistakes on credit records and requires that one's credit record only be provided for legitimate business, credit, or employment purposes.

Consumers may recover from reporting agencies (i.e., credit bureaus) and information users (i.e., potential or existing creditors) for both negligent and willful noncompliance. The law employs a "reasonableness" standard, under which suppliers and reporters of information may escape liability, even if the information supplied or reported is incorrect.[38] The FCRA, however, does not contemplate an unrelated third-party opening accounts in a victim's name and tying those accounts to an identity theft victim's established credit history. Before recent amendments, the FCRA effectively shifted the burden of avoiding identity theft away from parties in position to implement heightened controls (i.e., reporting agencies and users) onto unsuspecting consumers.[39]

In late November 2003, Congress and the President signed into law the Fair and Accurate Credit Transactions Act (FACTA). The law amends the FCRA by making it easier for consumers to protect themselves against identity theft and providing new legal rights to identity theft victims. The new law provides that:

- credit reporting agencies must fix erroneous information blamed on identity theft within four business days of receiving a police report and must inform the creditor who generated the inaccurate information;
- identity theft victims may get application and transaction data from firms that extended credit to identity imposters. This provision assists victims who often find they must do their own investigations before they can interest law enforcement in their case;
- credit grantors must take extra steps to positively identify an applicant if a "fraud alert" has been placed on a consumer's credit file. The new law is not specific, however, on just how credit issuers must confirm the identity of the applicants; and

- various measures be implemented to stop identity thieves from obtaining more credit using a victim's information once a victim reports the crime to authorities.[40]

The law does not take effect until late 2004.

One possible downside to FACTA is that it preempts many state identity theft laws. Various state laws that provide greater protection for identity theft victims may be nullified.

Third-Party or Downstream Liability

Since victims of identity theft are unlikely to recover from the thieves themselves, victims are increasingly looking to various third parties, including employers, for recovery for failure to protect their personal information. In fact, employment records are the primary source of all stolen personal information.[41] In the past two years, a few states—California, Washington, and Georgia—have enacted statutes that impose liability on holders of personal information, namely, employers.[42]

California has enacted sweeping legislation restricting the disclosure of personal information by businesses.[43] The state's Security Breach Information Act (SIBA) became effective July 1, 2003. The statute requires that any person or business "that conducts business in California and that owns or licenses computerized data that includes personal information, should disclose any breach of the security system following discovery or notification of the breach … to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." The phrase "conducts business in California" is not defined anywhere in the law but the almost certain import will be roughly equivalent to the "minimum contacts" standard applied in most civil litigation. Individuals and businesses located anywhere in the world that do business in California will be covered by the law.[44]

The term "personal information" is considered by the law to be an individual's first name or initial and last name in conjunction with any one or more of the

following social security number, credit or debit card number, in combination with any required access code or password that would allow access to an individual's financial account. Excluded from the definition of "personal information" is publicly available information that is lawfully made available to the general public from federal, state, or local government records.

The sanctions for violating the SBIA are strictly civil. Both individual and class action lawsuits may be filed under the law. The economic ramifications of the law, if not preempted by FACTA, will take many years to evaluate.

Surprisingly, no published court decision has yet resulted in an organization or employer paying damages to a third-party or employee victimized by identity theft. The legal underpinnings for such claims, however, are in place.[45]

Identity theft victims may sue organizations, both profit and non-profit, not only under various federal and state statutes, but under various common law theories. Claims for negligent hiring, retention, and supervision could provide one avenue of recovery. Under these recovery theories, 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. Such a legal standard may 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. Even if the employer had no reason to know that the perpetrator might engage in identity theft, the employer could still face liability for negligence in a lawsuit filed by victimized employees.[46]

Another viable theory of recovery when the employer itself authorized the disclosure of personal information and the disclosure resulted in identity theft is unreasonable disclosure of private facts.[47] This tort requires that private facts be

communicated to the public at large or that they become public knowledge. The information disclosed must be private in nature. Also, the disclosure must be highly offensive to a reasonable person.

By way of example, *Bodah v. Lakeville Motor Express, Inc.,*[48] is a class action suit filed by 204 employees against a trucking company. In the complaint, the plaintiffs alleged dissemination by fax of employee name and social security numbers to 16 terminal managers in six states. No precautions were taken to protect the confidentiality of the data. The Minnesota Supreme Court recognized that the social security number is a private fact whose unreasonable disclosure could support a claim for unreasonable disclosure of private facts. The case was dismissed only because the plaintiff employees failed to allege sufficiently broad publication of the private facts.

In another case, Ligand Pharmaceuticals in San Diego settled a negligence lawsuit brought by employees who were victims of identity theft. After Ligand merged with another company, personnel records on some of the acquired firm's employees were kept in a storage area. An employee found the box and used such data as names, birth dates, addresses and social security numbers to rack up credit card bills and rent apartments. Ligand settled the negligence case out of court for an undisclosed amount in the six figures.[49]

In another case, *Yutesler v. Sears Roebuck and Co.,*[50] a federal district court in Minnesota held that the Fair Credit Reporting Act does not preempt a common law claim for defamation of credit. Chase Bancard Services alerted Nicole Yutesler to a credit card account opened in her name. Yutesler did not open the account and reported the identity theft to major credit reporting agencies and the police. Yutesler's credit report showed a fraudulent Sears credit card account, among others. She and her attorney sent appropriate documentation, including a dispute letter and an affidavit of forgery to

credit reporting agencies. Experian (a credit reporting agency) deleted all of the disputed accounts from Yutesler's credit report except Sears. Subsequently, Sears rejected a settlement offer by Yutesler regarding Sears' treatment of the account. Yutesler sued Sears for violations of the FCRA and made a state common law claim for defamation of credit. The district court denied Sears' motion to dismiss the state law claim.

As the number of identify theft cases rises, the greater the risk of liability exposure for employers and other third parties. There are, however, numerous steps that both profit and non-profit entities can take to mitigate this risk.

Evaluate Internal Controls

Section 404 of the Sarbanes-Oxley Act of 2002 (SOX) requires management of a public company to include an assessment of the effectiveness of internal controls in the annual report. This assessment must be based on a framework of internal control that has been established by due process that allows for public comment. Most companies will use the framework developed by Committee of Sponsoring Organizations' (COSO) *Internal Control -- Integrated Framework*. COSO was originally formed in 1985 as an independent private sector initiative, which studied the causal factors of fraudulent financial reporting. The organization defined the attributes of internal control and developed recommendations for public companies and independent auditors, the SEC, and educational institutions.

One commentator notes that although SOX relates to publicly traded companies, many SOX requirements are going to be imposed on smaller, private companies by government customers, insurance companies, lenders, and others.[51] These firms may insist on adoption of SOX policies and procedures, including an evaluation of internal control. Thus, we suggest that even smaller companies should use the opportunity to evaluate information protection policies.

SOX assessment is directed at processes directly related to financial statement reporting including the maintenance of records that accurately and fairly reflect the transactions and dispositions of assets of the company. We contend that it is likely that a much broader evaluation will be necessary to provide management with the assurances required by SOX. Management should use the opportunity to assure that proper control is exercised over all assets, including information. Significant resources will be expended to comply with SOX requirements. Management should attempt to gain as much benefit as possible from the use of these resources. Evaluation of the security and privacy measures should be viewed as additional benefits.

Identify and Consider Objectives

Prior to any assessment of information security and privacy, every entity should establish the goals that should be achieved from the assessment. We believe that the basis of those goals can be addressed by considering the FTC's five core principles relating to information privacy. The principles are oriented towards consumers, but the concepts embraced relate to all stakeholders of an entity. Striving to meet these core principles will serve to satisfy most current laws and regulations as well as providing for the safeguarding of information assets. Core principles include:

> **Integrity/Security** -- Personal information should be collected and processed with controls to ensure that it is accurate. Additionally, it should be kept confidential and safeguarded when collected, processed, transmitted, and stored by the organization;
>
> **Access** --Consumers should have the ability to access their personal information, review it, and be permitted to provide corrections to inaccurate or incomplete data;
>
> **Notice** -- Consumers should be apprised of an organization's information police and practices before any personal information is gathered;
>
> **Choice** -- Consumers should be given an opportunity to consent or deny secondary uses of information collected for the primary purpose of the transaction. Ideally, the consumer should "opt in" to the subsequent use,

however, most organizations have used the "opt out" policy requiring consumers to tell them not to use their information for other purposes; and

Enforcement -- Consumers should be provided with recourse for violations of any of the other four principles.

Information Security and Privacy Controls

We address a number of the key controls that are often considered appropriate to provide for information security and privacy. These should not be considered all-inclusive, but should provide a basis for the evaluation of those security-related controls for many organizations.

Purge Outdated Records

A key element in the protection of information is the proper destruction of outdated materials. Proper, timely destruction of information is both a highly responsible and necessary business activity, one mandated by legal and regulatory requirements—as well as common sense—to protect consumers and businesses alike.[52] Although the media has cast suspicion on document shredding, due to the Enron scandal, states such as Wisconsin, California, and Georgia have enacted laws requiring the destruction of obsolete personal data. In addition, the GLB and HIPAA compel destruction of unnecessary records in the financial services and healthcare industries, respectively. Moreover, legal protection afforded to trade secrets by the Economic Espionage Act of 1996[53] necessitates that businesses have effective comprehensive procedures to destroy all discarded information.[54]

Given the image problems associated with discarding records, it is important to establish clear, well-structured information destruction policies and procedures. We suggest the following principles as the basis for any information destruction plan:

- **Have a Plan.** Following an appropriate plan will not only safeguard information assets but also stave off any concerns of impropriety that might subsequently arise from the destruction of specific documents;

- **Be Consistent In What is Destroyed**. Determine what should be retained and what should be destroyed and follow through with the procedures. Concerning the method of destruction, always erase files or destroy documents in an appropriate and similar manner. Relative to the timing of destruction, set appropriate periodic dates for destruction and keep to the schedule; and

- **Provide Documentation.** All policies, procedures, and schedules for destruction should be documented. Training programs should provide for and documentation should be maintained concerning the training of employees. Each destruction process should be documented and that documentation should be maintained and held until it can be assured that it will not be needed.[55]

Physical Control of Electronic Data Storage

Managers should track the acquisition, custody, and disposal of electronic data storage devices. This goes beyond tracking desktops, laptops, and servers; it includes other devices such as wireless handheld devices (e.g., Palm Pilot, BlackBerry) and newer miniature data storage devices such as StorCard (similar to a credit card and can hold up to 5 Gb), memory sticks, and miniature discs, to name a few.

Some say that tracking such devices is excessive and unnecessary, but consider the following situation. A former vice president of mergers and acquisitions for Morgan Stanley left the company and decided to sell his BlackBerry on eBay. A computer consultant bought the device for $15.50 and discovered more than 200 internal company e-mails from financial services firm Morgan Stanley and a database of more than 1,000 names, job titles (from vice presidents to managing directors), e-mail addresses and phone numbers (some of them home numbers) for Morgan Stanley executives worldwide.[56] The device also contained personal information from the previous owner including brokerage account numbers, mortgage payment information, and other bills such as credit card bills. This happened in spite of corporate policies and procedures that were in place including a contract signed by the owner whereby he promised to destroy or return proprietary information.[57]

Such an event does not appear to be an isolated incident. Two graduate students from MIT purchased 158 used disk drives (the majority from eBay) and found

personal information including credit card information (thousands of credit card numbers) and an enormous amount of e-mail and corporate financial information. Particularly surprising was one hard drive where it appeared that the hard drive was most likely used in an ATM machine in Illinois, and that no effort was made to remove any of the drive's financial information. The log contained account numbers, dates of access, and account balances.[58] The message here is clear: managers need to ensure that sensitive data is removed from all storage devices prior to their disposal.

File Encryption

Encryption adds another layer of protection. Like the technique used in spy movies, information is transformed using an algorithm and a secret key. The scrambled information can then be stored in a database with little risk of compromise. To retrieve the information, the reverse process (or decryption) is used to convert the scrambled data into intelligible information. Only those privy to the key can convert the data. Obviously, care must be taken to protect the key and to insure that the key is not lost.

Some database software packages have the built-in capability to encrypt and decrypt data during the storage and retrieval process. Those firms that lack sophisticated IT departments are advised to consider one of these packages.

Password Protection

Organizations should assure that only legitimate users have access to the computer network and associated data. Although passwords are the oldest line of defense they still constitute the most effective and efficient method of controlling access. Proper password use, however, is mandatory if control is to be maintained.

Some common password problems are easy to avoid. The most common password security problems relate to the use of "Joes." [59] Joes are account passwords that are variations of the account owner's personal information. The problem most often

results when users are first assigned default passwords, such as their last names, and then employees do not change them to something more secure.

Ideally, passwords should be randomly generated by a computer system and contain a combination of letters, numbers, and special characters. Employers should be prohibited from sharing their passwords with other users. Password security requires that they be changed periodically, but how often depends on the risks. Employees should not be permitted to display their passwords in a location where they could be seen by unauthorized individuals.

Firewalls

Firewalls are comprised of hardware and software that control the flow of data in to and out of networks. They must be established for networks available to external parties. Firewalls can examine and validate address information on all data packets, and then data can be passed to the appropriate application and screened again to grant access. Firewalls are necessary to help protect data stored on a network and are a major component in the overall protection of systems from unauthorized access. Policies and procedures should be in place to periodically evaluate and upgrade firewalls to incorporate current technology and to meet critical risks. However, since firewalls are basically locks, they are not foolproof (a key holder can open a lock, and there are similar risks for firewalls) as they can be bypassed through wireless computer access. Therefore, it is necessary to incorporate intrusion detection systems. Such systems can monitor (1) network traffic for potential hacking, (2) systems files for any changes by hackers, and (3) log files that may give evidence of intruders.

Maintain a Console Log

Each organization should maintain a log of each individual who has accessed files containing sensitive data. This creates an audit trail as to where a file has been sent. The monitoring of a console log can help an organization to detect promptly a

security breach. Downloading sensitive data to laptops or to computer or compact discs should be prohibited except with high-level approval.[60]

Control of Paper Documents

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.[61]

Employee Considerations

Evidence indicates that employees are responsible for almost half of the technology-related frauds. Thus, it is imperative that firms hire only the most trusted individuals for positions requiring access to customer and other stakeholder data. Internal controls should be in place to ensure that this is accomplished. Although various policies and procedures may prove useful, several specific controls are critical.

Background Checks

One internal control that helps prevent information theft is to conduct employee background checks. An individual with a history of perpetration of fraud schemes may move from one organization to another. When an employee background check is not done, a dishonest employee can steal vast amounts of personal information from an unsuspecting organization and move on to a new organization before the theft is discovered. Resumes should be scrutinized and information verified to determine that prospective employees graduated from the schools listed. Also, an organization should not rely on the telephone numbers listed on the resume for prior employers, as they may be false. Employer phone numbers should be checked by the organization independently.[62]

An additional technique is for organizations to do a second check of employment references six months after an employee starts work. The reason for a dishonest employee's recent dismissal from a previous job may not have had time to become part of the employee's record during the initial search.[63]

Create and Maintain an Information Security and Privacy Policy

An information security and privacy policy should be created, maintained, and enforced by every organization. Such a policy may be separate and distinct from a corporate ethics policy or a part of it. The policy should be clearly communicated to employees. Various avenues of communication include use in orientation of new hires, annual employee training seminars, and annual performance evaluations. Written acknowledgment by each employee that the policy has been read and understood should be required.

Even when an organization has established and implemented an information security and privacy policy, its employees still may be victimized by an identity theft. Any information security and privacy policy should include a contingency plan to help the organization react appropriately when a security breach occurs. An organization should consider contacting law enforcement upon first notice of a security breach. The organization should also notify all individuals whose personal information may have been purloined.[64]

Mandatory Vacations

Specific schemes to siphon off and sell personal information typically require constant attention by the employee to avoid detection. It is good policy to require all employees to take vacations for fixed periods of time. This internal control is an effective deterrent and detective device for frauds in addition to identity theft and considered important particularly in financial institutions. For example, all officers of FDIC-insured banks are required to take two consecutive weeks of vacation per year. It is important

that coverage of substitute employees for those on vacation include the employee's "high risk" tasks.

Hotline

A hotline should be established so that employees can report suspicious activity anonymously. This control can be effectively outsourced at reasonable cost. The contract telephone number should be "advertised" by posting it prominently in the work place. This control not only has the potential for uncovering security-fraud activities, it is a strong deterrent. One downside to this control is that employees have been known to report fictitious tips to retaliate against another employee. This risk, however, is a small cost relative to the potential costs of data theft.

Conduct a Threat Analysis

A threat analysis that examines an entity's exposure to information theft should be performed. This includes an assessment of what personal information databases are held and how they could be compromised. The purpose of a threat analysis is to "outsmart the crooks." A threat analysis can help to direct an internal audit plan for information security and privacy and in particular, highlight the most vulnerable databases. Consideration of each type of database and the evaluation of the exposure to loss or compromise helps management to see what the information thief sees. Steps then should be taken to eliminate, minimize, or at least control the exposures.

Consider Insurance as a Risk Management Tool

Insurers have developed "cyberinsurance" or "e-risk insurance" as a viable risk management tool. Various insurers including Lloyd's of London, American International Group, and Cigna, offer protection that often encompasses losses caused by the inadvertent release of confidential data.[65] Traditional business hazard insurance does not cover cyberlosses. Premiums for e-risk insurance are estimated at $10,000 to $50,000 for a $1 million policy.[66]

Conclusion

Identity theft is one of the fastest growing crimes of the twenty-first century. The fallout from identity theft includes not only victims having to clear up fraudulent bank accounts and credit card debts, but increased public risk as identity theft is linked to drug trafficking, money laundering, and terrorism. Identity theft is accomplished through both low-tech and high-tech methods.

Organizations that do not take proactive steps to minimize the likelihood of identity theft risk increased liability exposure. Since identity theft victims are not likely to recover from thieves, victims are increasingly looking to third parties, including corporations and government agencies, for recovery for failure to protect personal information.

Numerous federal laws apply to identity theft including ITADA, FAFI, HIPAA and the FCRA. State statutes and common law claims (not preempted by FCRA) also are available to identity theft victims. The legal underpinnings for third-party or downstream liability are in place.

Organizations can take numerous steps to minimize the risk of identity theft. One step is a thorough evaluation of internal controls. Every entity should establish the goals that should be achieved by such an internal control assessment. The goals should be based on the FTC core principles of security, access, notice, choice, and enforcement.

Numerous controls can facilitate enhanced information security and privacy. A key control in information protection is the proper destruction of outdated materials. Managers should also track the acquisition, custody, and disposal of electronic data storage devices. Other significant controls that help prevent information theft are file encryption, password protection, employee background checks, creation and maintenance of an information security and privacy policy, maintenance of a console log,

control of paper documents, mandatory vacations, establishment of a hotline, and performance of a threat analysis.

Widespread implementation of the controls outlined in this article would accomplish two objectives. First, it is likely that the frequency and severity of occurrences of identity theft would both be reduced. Second, organizations would diminish their potential liability exposure, both criminal and civil, for loss of confidential personal information and subsequent identity theft events.

Endnotes

[1] Identity theft must be distinguished from identity fraud. The latter is a broader term that refers to the criminal use of false identities or fraudulent identification documents. Identity theft is limited to the use of the means of identification of another person. A prime example of identity fraud is the 9/11 terrorists who procured drivers licenses in their own names using false addresses supported by fraudulently obtained identification documents. Identity theft is too narrow a concept to capture the divers uses of false identities and false identification documents. U.S. Senate (2002) 'The Financial War on Terrorism and the Administration's Implementation of the Anti-Money Laundering Provisions of the USA Patriot Act: Hearing Before the Senate Comm. On Banking, Housing, and Urban Affairs,' statement of Michael Chertoff, Assistant Attorney General; Willox, N. and Regan, T. (2002) 'Identity Fraud: Providing a Solution', Lexis-Nexis, March, pp. 1-17.
[2] Surmacz, J. (2003) 'Losses from Identity Theft to Total $221 Billion Worldwide', May 23, http://www.csoonline.com/metrics/viewmetric.cfm?id=551
3 Federal Trade Commission (2003) 'FTC Offers Tips to Help Guard Against Fraud', Consumer Financial Services Law Report, February 14.
[4] DeMarrais, K. (2003) 'Identity Theft on the Rise, FTC Warns', Knight Ridder Business News, September 4, pp. 1-4.
[5] Schaefer, S. (2003) 'Identity Theft Costs Businesses $48 Billion a Year', Wall Street Journal, September 4, p. D2.
[6] See reference 4 above.
[7] Cringely, R. (2003) 'They've Got Your Number', Inc., August, pp. 61-2.
[8] Fikes, B. (2003) 'Identity Theft Hits Millions of Americans', Knight Ridder Business News, September 4, pp.5-6.
[9] Couch, C. (2002) 'Forcing the Choice Between Commerce and Consumers: Application of the FCRA to Identity Theft', Alabama Law Review 53, pp. 583-597.
[10] Collins, J. (2003) 'Business Identity Theft', Journal of Forensic Accounting 4(2), pp. 303-306.
[11] Lormel, D. (2001) 'Prepared Remarks Before the House Committee on Financial Services, hearing on "Dismantling the Financial Infrastructure of Global Terrorism"', October 3, p. 6.
[12] See reference 4 above.
[13] MyFico.com (2003) 'How to Guard Against Identity Theft', Credit Health Newsletter, December.
[14] Ibid.
[15] Ibid.
[16] U.S. v. Massey, No. 99-60116-01-AA (D. Or. Oct. 6, 2000); U.S. v. Melton, No. 99-60118-01-AA (D. Or. July 19, 2000).
[17] Hoar, S. (2001) 'Identity Theft: The Crime of the New Millennium', Oregon Law Review 80 (4), pp.1423-1447.
[18] Pub. L. No. 105-318, 112 Stat. 3010 (2003)(codified at 18 U.S.C. §1028).
[19] Pub. L. No. 105-318, 112 Stat. 3010 (2003) (codified at 18 U.S.C. §1028(a)(7)).

[20] Pub. L. No. 105-318, 112 Stat. 3010 (2003)(codified at 18 U.S.C. §1028(d)(4)).
[21] Pub. L. No. 105-318, 112 Stat. 3010 (2003)(codified at 18 U.S.C. §1028(d)(4)(A)-(D)).
[22] Pub. L. No. 105-318, 112 Stat. 3010 (2003)(codified at 18 U.S.C. §1028(b)(1)(D)).
[23] The website can be found at http://www.consumer.gov/idtheft and the FTC Identity Theft Hotline is 877-IDTHEFT. The FTC Identity Theft Clearinghouse is located at 600 Pennsylvania Avenue, N.W., Washington, D.C. 20580.
[24] 75 Fed. Appx. 392 (6th Cir. 2003).
[25] 346 F.3d 22 (2d Cir. 2003).
[26] Pub. L. No. 106-102, 113 Stat. 1436 (2003)(codified at 15 U.S.C. §§6801-6827)).
[27] See reference 17 above.
[28] 16 C.F.R. §314.3(a).
[29] 16 C.F.R. §314.4.
[30] Benoit, M. and Lovoy, E. (2003) 'Update on Consumer Financial Privacy Legislation and Regulation', Business Lawyer 58, pp. 1163-1179.
[31] Ibid.
[32] Pub. L. No. 104-191, 110 Stat. 1936 (2003)(codified at 42 U.S.C. §§1320 et. seq).
[33] Levine, R. (2003) 'HIPAA: Data Trade Prosecutions on the Horizon?,' Business Crimes, October 12, pp. 1-6.
[34] Pub. L. No. 104-191, 110 Stat. 1936 (2003)(codified at 42 U.S.C. §1320d-6).
[35] Pub. L. No. 104-191, 110 Stat. 1936 (2003)(codified at 42 U.S.C. §1320d(6)).
[36] Pub. L. No. 104-191, 110 Stat. 1936 (2003)(codified at 42 U.S.C. §1320d-6(b)).
[37] Pub. L. No. , (codified at 15 U.S.C. §§1681-1681t).
[38] See reference 9 above.
[39] Ibid.
[40] Sullivan, B. (2003) 'Help on the Way for ID Theft Victims,' MSNBC News, November 26, http://msnbc.com/news/998144.asp.
[41] Gray, M. (2003) 'The New Identity Crisis', Corporate Counsel, December 15, pp. 57-60.
[42] Ibid.
[43] California Civil Code §1798.82 et seq. (2003).
[44] Treglia, S. (2003) 'One State's New ID Theft Act Has Worldwide Implications', New York Law Journal, July 15, pp. 5-8.
[45] Solomon, T., Gordon, P., and New, L. (2003) 'Incidence of Workplace Identity Theft Signals Need for Proactive Measures', New York Law Journal, December 15, pp. 9-10.
[46] Ibid.
[47] Ibid.
[48] 663 N.W.2d 550 (Minn. 2003).
[49] Armour, S. (2003) 'Employment Records Prove Ripe Source for Identity Theft', USA Today, January 23, p. B1.
[50] 263 F.Supp. 2d 1209 (D. Minn. 2003).
[51] Klingenberg, D. (2003) 'Who's Winning the Sarbanes-Oxley?', Nashville Business Journal, September 16.
[52] Geiser, W. and Johnson, B. (2002) 'A Brave New World', The Information Management Journal, Nov./Dec., pp. 47-52.
[53] Pub. L. No. 104-294, 110 Stat. 3488 (2003)(codified at 18 U.S.C. §§1831 et seq.).
[54] See reference 52 above.
[55] Ibid.
[56] Zetter, K. (2003) 'Blackberry Reveals Bank's Secrets', Wired News, August 25, http://www.wired.com/news/business/0,1367,60052,00.html.
[57] Ibid.
[58] Garfinkel, S.L. and Shelat, A. (2003) 'Remembrance of Data Passed: A Study of Disk Sanitization Practices', IEEE Security & Privacy, January/February.
[59] Graves, J. and Torrence, K.H. (1997) The CPA's Guide to Information Security, Kent Information Services, Kent, Ohio.
[60] See reference 45 above.

[61] Ibid.
[62] Hillison, W., Pacini, C., and Sinason, D. (1999) 'The Internal Auditor as Fraud-Buster', Managerial Auditing Journal 14 (7), pp. 351-362.
[63] Ibid.
[64] See reference 45 above.
[65] Chuvakin, A. (2001) 'Your Money or Your Life! Which Would You Rather Lost to Hackers: Private Customer Data or Your Website?, June 25, http://www.securitywatch.com/RES/June25.html.
[66] Groves, S. (2003) 'The Unlikely Heroes of Cyber Security', The Information Management Journal, May/June, pp. 34-40.