SecurityManagement ONLINE
The Security Professional's Central Web Connection

Identity Theft

December 2001

How to Avoid an Identity Crisis

By Robert J. Del Grosso

Businesses can win the esteem of their employees and improve the bottom line by helping staff prevent or deal with identity theft.

Michelle Brown would probably be called a good role model. Lacking the money to study beyond high school, at age 15 she took after-school jobs to finance a college education. After graduation, she got a job in international banking, proving a steady, hard-working presence at her firm. Since first establishing credit at age 17, she maintained a stellar credit history for 11 years. She never had any trouble with the law. That exemplary record came crashing down on January 12, 1999, through no fault of her own.

On that day, Brown received a call from a Bank of America representative asking why she hadn't made the first payment on a truck she had bought the previous month. She had made no such purchase. She immediately placed fraud alerts on her credit reports and on her driver's license number, and she cancelled all her credit cards.

It was too late. An imposter who had assumed her identity from January 1998 to July 1999 had already rung up more than $50,000 in goods and services: cellular service, utilities, rental properties, and much more--even liposuction. Worse, this doppelganger had obtained a fraudulent driver's license in Brown's name. When the woman was arrested for trafficking 3,000 pounds of marijuana, she presented herself as Brown. For the first half of 1999, the woman was a fugitive cloaked in Brown's identity, and Brown herself was terrified of being arrested. Even when the imposter was caught in July 1999, she was booked into the prison under Brown's name.

Only after 500 hours of legwork and pleading with creditors and law enforcement and corrections authorities did Brown restore her good name and credit. But the crime has left a scar. As Brown testified last year before the Senate Judiciary Committee's Subcommittee on Technology, Terrorism, and Government Information: "I faced many difficulties in clearing my name, and I still face the fear that I will forever be linked with the perpetrator's criminal record."

Brown's odyssey is repeated more and more frequently as criminals find that identity theft is low risk and high yield. Though identity theft is not a corporate issue per se, a victim/employee struggling to clear his or her name will be distracted at work and lose productivity. By developing an awareness of identity theft and setting up a program for assisting victimized employees, security managers can contribute to restoring both the employee's morale and effectiveness at work.

Businesses can take many specific actions to help employees who are or may become victims. But the first step is for the security team itself to understand how these schemes work.

How it works.
Identity theft occurs when a thief steals someone's personal, financial identifying information. With the victim's personal data (including name, address, phone number, date of birth, Social Security number, and bank account data), the thief assumes the victim's persona in dealings with such creditors as

vendors, credit card companies, and financial institutions.

Methods of identity theft include stealing a wallet, shoulder surfing, and simply submitting a change of address form to divert a victim's mail to a criminal's mail drop. Dumpster diving, in which a thief goes through garbage, can be an effective means of harvesting reusable information from household trash or from the alleyway behind a restaurant or store. Dishonest employees at work sometimes parlay their access to a coworker's sensitive, personal information into their own financial gain by selling this information to identity thieves or by misusing it themselves. In Michelle Brown's case, the thief pilfered Brown's rental application, which contained her Social Security number and other sensitive data, from her landlord's property management office.

Another major exposure is incoming mail, especially unsolicited and unexpected pre-approved credit card offers. If that mail is stolen, the employee will never be aware of its existence and would have no reason to suspect mischief. Outgoing mail is also at risk. For example, a completed credit card application contains someone's most closely held personal identifiers--the complete data needed to take over someone's identity. Mail theft also provides a built-in head start for the thief, since the fraud is typically only discovered long after funds have been diverted.

Less common is high-tech identity theft, though it still poses a significant threat. For example, using a scanning device attached to an automated teller machine (ATM) or even a sham ATM, the identity thief might "skim" someone's coded identifying data from the magnetic strip of an ATM card or credit card and reproduce it on a blank card so the data becomes machine readable. (In some areas of the country, thieves are reproducing this data on electronic hotel room keys so that they won't be caught carrying around large numbers of credit cards.)

In other high-tech ploys, victims innocently respond to spam that promises money or prizes. They are prompted to enter identifying information to become eligible for a reward, though the fraud artist has no intent to deliver any such prize. Once the victim's biographical information is obtained, a thief establishes a parallel universe of credit and runs up expenditures unbeknownst to the victim.

Identity theft is so devastating because it goes undetected for so long. On average, according to Beth Givens, director of the Privacy Rights Clearinghouse, a consumer advocacy organization dedicated to privacy rights, it takes 14 months for a victim to discover that his or her identity has been stolen. Some schemes go undetected for years because thieves are savvy enough to initially repay debts to obtain even larger credit limits.

Damage may be compounded by the limited law enforcement response. While greater investigative resources are being brought to bear, law enforcement's attention to identity theft is not yet commensurate with the crime. These cases compete for the attention of investigative personnel with traditional forms of fraud, such as securities fraud, which involve greater losses.

Extent.
The exact extent of identity theft is unknown; figures quickly become outdated. In a July 2000 hearing before the Senate Subcommittee on Technology, Terrorism, and Government Information, Givens estimated 500,000 to 700,000 victims of identity theft nationally in 2000. In the June 2001 edition of *SAR Activity Review*, between December 1, 2000, and April 30, 2001, financial institutions filed 352 suspicious activity reports relating to identity theft, a 50 percent increase from the same period a year before. In 1998, the U.S. General Accounting Office reported a 15-fold increase in identity theft complaints received by a leading credit reporting bureau over the prior five-year period.

Last year, Jeffrey Klurfeld, director of the Western Regional Office of the Federal Trade Commission (FTC), reported that the three states with the largest number of identity fraud complainants are California, New York, and Florida. The FTC further reported that 16 percent of all identity theft complainants reported the loss of more than $10,000.

The incidence of identity theft is expected to increase as junk mail proliferates and the Internet expands. For example, credit card offers, financial statements, and other sensitive documents, when not properly disposed of, are a prime source of easily stolen financial data. According to Givens, in

1998 alone, it was estimated that 3.5 billion pre-approved offers of credit were unilaterally extended to consumers in the mail. The thieves themselves realize that this crime is straightforward, profitable, and unlikely to attract investigative scrutiny or lengthy jail terms. And as more banks go online and as companies share private data with partners and associated businesses, the risk of hacker compromise or insider theft goes up.

Identity theft can strike anyone. Even Tiger Woods has been victimized. His Social Security number was hijacked by a stranger, who then qualified for credit cards under Woods's name. In many cases, the thief disappears when discovered. In the Woods case, perhaps because of the high-profile nature of the victim, the culprit was caught and arrested, but not before he spent $17,000 on such items as a 70-inch television. (The thief, a repeat offender and subject to California's "three strikes" law, was convicted and sentenced to 200 years in prison in April.)

Impact.
The FBI has reported that the most frequent uses of identity theft have been to obtain new credit cards, use or change an existing credit card account, obtain cellular telephone service, open new bank accounts, and borrow money. The ensuing losses can be significant.

Fraudulent expenses and loans can cripple a victim's credit rating if, for example, an otherwise unknown account is opened in a victim's name or an existing account is taken over for the thief's own enrichment. Sizeable unauthorized financial obligations might then be incurred but never paid. Each delinquency would be held against the victim's own credit history until corrected. The victim might not be aware of this activity for months.

The impact on a victim's life can be staggering. With horrible debt and creditors banging at the door, the victim may be denied a job opportunity, a mortgage, or a loan. Checks may bounce, so landlords, utilities, financing companies, and other service providers could terminate services. Even less obvious, but still instrumental, services and activities could be threatened, if, for example, a university bursar's check or child-care provider's check bounces.

In one instance documented by the U.S. Department of Justice, a convicted felon assumed a victim's identity and racked up debt, including getting a federal home loan, putting $100,000 on credit cards, and purchasing houses, handguns, and motorcycles, in the victim's name. The perpetrator even taunted the victim over the phone. He then filed for bankruptcy in the name of the victim. It took more than four years and the personal expenditure of over $15,000 by the victim to restore his good name and credit.

Beyond the financial loss (some of which may be covered by credit card companies) are the monumental hassles involved with restoring good credit and the psychological trauma caused by the sense of invasion of personal space. Merely by donning someone's personal identifiers, a thief can undo the lifetime effort of establishing a hard-earned credit reputation and financial stability. Victims continue to suffer as their struggles to re-establish their name and credit history re-open these wounds time and again.

Prevention.
While identity theft can never be eradicated, certain precautions can limit its occurrence. Companies should be aware of these. Precautions include careful handling of personal information and periodic review of credit reports.

Prudence. Caution is critical when sharing ID information. Sensitive information should only be given to someone with a legitimate "need to know." The consumer must decide whether there is a way to provide comparable information without disclosing sensitive data. If not, the consumer should determine how the data will be used and to whom it may be disseminated. One should never give out his or her Social Security number or use it as a means of identification unless it is required by a person or business known to be legitimate, such as a bank or a healthcare provider. Over the phone, personal and financial information should only be given out if the employee has initiated the call. Similarly, such information should not be placed on the Internet. The best approach is to deal with vendors with a track record of reliability.

In addition, one should never place outgoing mail in one's own mailbox, which is typically accessible to thieves. A much more secure bet is using a postal service mailbox or going directly to the post office. Unnecessary or out-of-date credit receipts, financial statements, and the like should not be discarded intact but should instead be shredded first.

Document review. To cull out any discrepancies, bills and monthly statements should be reviewed and reconciled. This may sound unrealistic for those many people who don't even balance their checkbooks, but it is one of the best ways to identify signs of theft. For example, the receipt of bills for accounts that were never opened or the listing of previously unknown debts or charges on credit card statements are two of the indicia of identity theft.

Another warning sign is when credit or bank statements are not received on time; a thief may have had the victim's mail sent to the thief's own address. Failure to report this aberration provides a thief with an even greater head start to run up charges.

In addition, everyone should periodically order copies of and analyze their credit reports in search of fraudulent accounts, unauthorized purchases, or false information. Performing such an inspection annually, even absent a hint of identity theft, will minimize exposure.

Copies of relevant financial records should be retained for at least one year to preserve the necessary documentation to reconstruct a person's financial history should an identity theft occur in the future.

Role of business.
Victims have the primary responsibility for clearing and maintaining the accurate and complete record of their own financial history. But victimized workers may not know how or where to turn to for support or direction. That's where a security department can help.

To see how companies are addressing this issue, the author informally polled the security directors of 12 corporations and consulting firms. Participating companies ranged from 15 to 120,000 employees and were engaged in, among other fields, manufacturing, retailing, pharmaceuticals, and aerospace. While none of the respondents has a formal identity theft program, they all address the problem on an ad hoc basis.

For example, at some companies security personnel respond to occasional informal requests for individual assistance. One company noted that on occasion it has established contact with an employee's credit card company or bank as a service. In those cases, the theft of an employee's corporate identity was recognized as a security responsibility and was addressed appropriately.

Only one company responding to the survey provides identity theft overviews and training at new employee orientation. Others interviewed said that they have only limited programs. One survey respondent noted that it has an ongoing training resource in an executive who was a victim of identity theft himself. But none of the companies polled covers identity theft at annual training.

Companies can do much more. They can help staff by creating awareness programs and directing employees to legal, regulatory, and organizational resources. They can provide employees with plans of action for dealing with identity theft (see **sidebar**, page 76).

Awareness programs. Security could work with the human resources (HR) department to distribute handouts on identity theft or publish material in the company's newsletter. The departments might also periodically place a summary of identity theft risks on company bulletin boards. If it hasn't done so already, HR could use training conferences, workshops, or departmental meetings to educate the work force on the nature of identity theft as well as ways of combating it. Through these communication venues, HR can effectively field inquiries and guide concerned employees.

A compliance program should mention the need for employees to limit access to sensitive third-party personal information. By reason of their job responsibilities, certain employees have "a need to know" this information. However, authorized personnel should be periodically reminded of company policy not to divulge this information without a legitimate business reason and not to do so for personal

gain. Universal enforcement and documentation of each initiative to republish this provision will limit problems and will provide an employer with a viable defense in case of litigation. Any corporate awareness program should also address the identity theft or compromise of a corporate identity, as would occur with the theft of a corporate credit card.

Another option is to establish an identity theft page on an intranet site or to add it to the security department's Web page, if one exists. As a model, companies might emulate what they do to help business travelers keep safe on the road: provide an ongoing blueprint for employees to follow if they have been victimized. The page can include information about reporting the theft and guidance on avoiding subsequent incidents. It can offer tips, such as the need to check credit reports annually.

The Web page would be accessible to all, and it could be easily updated as necessary. This would provide employees with ongoing guidance and would reduce the burden on security personnel.

Legal recourse. The federal government and many states have criminalized identity theft, but employees may not know where to begin. Businesses can help victims of identity theft seek the state's help in prosecuting perpetrators. In addition, businesses can help their employees seek assistance from the FTC and other bodies with online presences.

Statutes. Various statutes establish criminal penalties for identity theft. On the federal level, the Identity Theft and Assumption Deterrence Act of 1998 makes it a federal crime when someone: "knowingly 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."

This law includes the criminal misuse of Social Security and other government identification numbers, unique biometric data, and electronic access devices and routing codes used in the telecommunication and financial sectors.

The act sets a maximum sentence of 25 years (depending on enumerated factors) plus restitution, fines, and the potential forfeiture of any personal property used in the commission of the crime. When prosecutors can prove the elements of similar offenses, including mail, wire, and credit card fraud, they will add those charges to the ID theft charges.

Kimberly Guadagno, a former federal prosecutor in New Jersey who is now in private law practice, explains that the identity theft statute is succeeding--more criminals are being prosecuted because of enhanced criminal penalties. "What was once considered no more serious than a traffic ticket is now treated as a felony with possible prison terms," according to Guadagno. That's happening nationwide. Unfortunately, this message hasn't really made it to the street yet, so incidents are still on the rise.

On the state level, more than 30 states have enacted specific "theft of identity" laws. Other states, such as New York, lack statutes targeting identity theft per se, but they address the issue through companion statutes. For example, in cases of identity theft, New York prosecutors commonly charge suspects with related crimes that are on the books, such as use of another's credit card, impersonation of a victim, or larceny by false pretense. New York is also typical of many states in that it has an informative Web site (which, like all Web sites mentioned in this article, can be reached via *SM Online*) and a designated representative from its Attorney General's office (800/771-7755) who can provide guidance on identity theft issues.

Consumer protection is provided by the Fair Credit Reporting Act, which regulates credit reporting agencies and makes them responsible for correcting inaccurate information in credit reports and for deleting disputed information that cannot be verified. The Fair Credit Billing Act of 2000, which amended the Truth in Lending Act, provides for the correction of billing errors and establishes liability limits for fraudulent credit card use. However, the protection of the FDIC's coverage of $100,000 per ownership category at each insured institution does not apply to identity theft. This protection is provided only for monies in deposit and only if the federally insured bank or savings institution fails.

Other resources. Victims also have recourse with the FTC. That body's stated mission is "to promote the efficient functioning of the marketplace by protecting consumers from unfair or deceptive

acts or practices and increasing consumer choice by promoting vigorous competition."

In part, the FTC fulfills this responsibility by serving as the federal clearinghouse for victims of identity theft and by offering expert information on identity theft. The FTC also publishes guidance in the form of complimentary "how to" publications (such as *Identity Crisis...What to Do If your Identity Is Stolen* and *Identity Thieves Can Ruin Your Good Name: Tips for Avoiding IT*). The FTC has an identity theft Web site and a toll-free "IT Hotline": 877/IDTHEFT.

Other agencies with Web sites on identity theft are Justice, the FBI, the Secret Service, and the Postal Inspection Service.

The Privacy Rights Clearinghouse, a leading, nonprofit consumer information and advocacy group, also has valuable information on its Web site. It contains fact sheets on a range of issues: how to organize an identity theft case, how to enhance victim-investigator relations, and how to overcome the emotional impact. The site also contains stories from victims and links to related sites. An affiliated site, the ID Theft Center, contains a host of other resources, including frequently asked questions on topics such as establishing local support centers.

A distracted employee is an unproductive employee. Providing assistance to employees in identity theft matters benefits everyone involved. It makes financial sense for the business. And it will likely earn the appreciation and loyalty of staff.

Robert J. Del Grosso is director of investigative services with the accounting firm of Margolin, Winer & Evens in New York. He is a member of ASIS. The Web sites mentioned can be reached via SM Online*. Click on "Beyond Print" and scroll to "Identity Theft."*

Self-Help for ID Theft: Plan of Action

Victims typically don't know how they can help themselves or how they can begin to resurrect their good name. While this is a time-consuming process (estimated to take 175 hours on average over a two-year period, according to Beth Givens of the Privacy Rights Clearinghouse), corrective action must be initiated.

The "plan of action" below can be used by any employee. It can rule out potential problems or prevent further loss and restore a person's credit reputation if his or her identity has already been stolen. The points of contact might also limit out-of-pocket loss and time expended to restore an employee's credit rating. These contacts can provide guidance in the correction of erroneous information on an ongoing basis.

If you have reason to believe that your identity has been stolen, immediately do the following:

1. Contact the fraud department of each of the three major credit bureaus. Inform them of the basis of your concern. Ask them to "flag" your file: This will ensure that creditors get your approval before any new account is opened in your name or a change is made to an account. Ask how long this "flag" will automatically be maintained and how it can be extended. Confirm your conversations in writing: Send a letter to each credit bureau stating whom you spoke to, when, what was discussed, and any promise of follow-up action made to you. Send copies of your documentation. Do not send original documents; keep a copy of your letter. Send your package via registered or certified mail with return receipt requested. Keep a continuing log of your conversations and retain copies of all correspondence.

Obtain your credit report from each credit bureau (it is free if it is inaccurate due to fraud). Review each report to see whether any other fraudulent account has been opened in your name, and demand that each fraudulent account be closed immediately.

Legal representation could be necessary if creditors or credit reporting agencies ignore requests to remove fraudulent entries from your credit history or if they have been negligent in tarnishing your

credit record. Restitution is another civil remedy that could be considered if the thief is ultimately apprehended.

2. Contact the creditors for any accounts that have been tampered with or opened fraudulently; speak to someone in the security or fraud investigation department. Confirm your conversation in writing--charges can accrue unless you notify credit card companies promptly. Close compromised accounts and stop payment, if appropriate. Use different personal identification numbers (PINs) and passwords to open a new account.

3. File a complaint with the police in the area where the theft took place. Obtain a copy of the complaint; banks and credit card companies may require one. Be polite but persistent in reporting the complaint to the police; otherwise they may be reluctant to issue a report. Contact the U.S. Postal Service if personal mail has been stolen.

4. Contact the Federal Trade Commission (FTC), which will provide information and guidance to help to avoid and resolve financial problems caused by identity theft. The FTC publishes excellent informational brochures on how to deal with identity fraud, which can also be downloaded.

Contacting Credit Bureaus

Equifax
To report fraud: 800/525-6285, or write: Equifax, Office of Fraud Alert, P.O. Box 105069, Atlanta, GA 30348.

- To order a copy of your credit report, write to P.O. Box 470241, Atlanta, GA 30374, Attn.: Disclosure Department. Or call 800/685-1111. Or visit the Web site (available, as are the sites of the other two credit bureaus, via *SM Online*).
- Disputes of information in the report must be done in writing and sent to: Equifax Service Center, Attn.: Dispute Department, P.O. Box 740256, Atlanta, GA 30374.
- To remove your name from pre-approved offers of credit and marketing lists, call 888/567-8688 or write to Equifax Options, P.O. Box 740123, Atlanta, GA 30374-0123.

Experian (formerly TRW)
To report fraud: 888/EXPERIAN (listen to choices). Or write: Experian, Consumer Fraud Assistance, P.O. Box 1017, Allen, TX 75013.

- Copies of credit reports can be ordered by logging on to Experian's Web site and selecting United States, calling 800/311-4769, or writing to P.O. Box 9600, Allen, TX 75013. The report costs $8.50 in most states. You must provide full name, home address (previous addresses for the past 5 years if different from the current address), date of birth, Social Security number, and two pieces of address identification, such as utility bills, if you have moved in the past two years.
- To dispute information in a credit report, call 800/493-1058 or write P.O. Box 9556, Allen, TX 75013.
- To remove your name from pre-approved offers of credit cards, call 800/567-8688. To remove your name from other marketing lists, call 800/407-1088.

TRANS UNION
To report fraud: telephone: 800/680-7289; fax: 714/447-6034; or write: Fraud Victim Assistance Dept., Fullerton, CA 92834.

- To obtain a copy of your credit report, write to Trans Union LLC, Consumer Disclosure Center, P.O. Box 1000, Chester, PA 19022, or go to the Trans Union Web site. You must provide full name, home address (previous addresses for the past two years if different), current employer, date of birth, Social Security number, and two pieces of address identification if you have moved within the past two years.

- To dispute information on a credit report, call 800/916-8800.
- To have your name removed from pre-approved offers of credit and marketing lists call 888/5OPTOUT (888/567-8688) or write Trans Union LLC's Name Removal Option, P.O. Box 97328, Jackson, MS 39288-7328.


back to Security Management Online