



Stopping ID Theft in Its Tracks

by Lynne Sanders

Identity theft, the fastest growing crime of the 21st century, can be devastating to anyone touched by it. Victims can spend years trying to repair their damaged credit, and banks often expend countless hours assisting customers and noncustomers alike in the repair of their accounts and financial standing. Handled improperly or without the right degree of sensitivity, banks stand to lose their customer's trust, and the implication for reputation risk is enormous.

ID theft occurs when someone co-opts a consumer's personal identifying information, such as name, address, Social Security number, or credit card numbers, and uses the data to represent himself or herself as that person for fraudulent purposes. This crime has grown to such epidemic proportions due largely to the fact that in performing such daily activities as writing checks or using a debit or credit card, consumers reveal personal information that, in the wrong hands, can be used for illegal purposes. Factor in the escalating use of the Internet, and the amount of personal data available for the taking increases exponentially. Thieves with the right skill-set can hack into Web sites and obtain enormous amounts of data, all under anonymous cover.

When a thief obtains personal identifying data, that information can be used in

a variety of ways. An ID thief can establish telephone or cellular service or obtain a credit card, revolving credit line, or other type of credit. With credit established, a thief can run up exorbitant bills with no intention of repayment, in the process totally destroying the victim's credit history.

The Federal Trade Commission, the lead governmental agency addressing identity theft, launched an ID Theft hotline and data clearinghouse in 1999. For the year 2000 the FTC processed more than 40,000 reports from consumers and victims of identity theft. Approximately 64 percent, or 26,000, of these complaints were incidents in which an identity theft occurred. Of the identity theft complaints received, about 50 percent related to credit card fraud where a new card was opened or existing cards were used for unauthorized charges.

Thanks to federal laws that have existed for many years, victims of credit and banking fraud are generally liable for no more than the first \$50 of a loss. It is therefore in the best interests if the banking community to safeguard our customer's information. While recent legislation and media attention has raised awareness of privacy issues, the idea of safeguarding customer information is not new to financial institutions. Banks use a combination of safeguards to protect personal information, such as

security standards, strict privacy policies, robust fraud detection practices, and employee training.

Although victims of identity theft may not be burdened with the financial charges, the personal and emotional pain is enormous. Victims face a frustrating, emotionally draining process of regaining their financial health, a process that can take years. Consumers can minimize their risk of becoming victims of this crime by managing their personal information wisely. There are precautions one can take to guard against identity theft and specific procedures to follow should an identity theft occur (see page 37). Educating customers is one of the most important things a financial institution can do to help curb ID theft.

Banks, law enforcement, and the financial services industry as a whole continue to work toward minimizing the crime of identity theft. Advanced technology, such as biometrics, adoption of stricter state laws, and sharing of victim information, are a few of the new tools in use today to combat this growing problem. While identity is not likely to be completely eviscerated, collectively the banking industry is striving to minimize the effect of this crime on customers.

Banks across the country are fighting ID theft in a number of ways. For a lucky

Illustration by Ace Layton

Banks use a combination of safeguards to protect personal information, such as security standards, strict privacy policies, robust fraud detection practices, and employee training.

few, the problem hasn't risen to crisis proportions, but it is a growing problem.

Detective Lynn Weddle of the Topeka (Kansas) Police Department, indicates that what many bankers have thought of for years as "fraud" is actually a form of identity theft. In the first 12 months since identity theft was criminalized in 2000, Topeka, a town of 119,000 people, has had more than 100 reports of ID theft. Weddle estimated that more than twice that number of cases are discovered by detectives and sent to the court, though not reported by the victims as ID theft. "If a party signs my documents for economic gain," she said, "that's forgery, but if that party uses my information on a check for economic gain — regardless of whose account is involved — that's ID theft."

At Topeka's largest local bank, Commerce Bank and Trust (CB&T), senior vice president Linda Woodland, and vice president Betty Seimears, indicated that ID theft has not yet been a major problem; however, the bank is paying careful attention to the issue. Calls concerning identity theft are directed to one specific individual, who, working with the bank's security department, assists customers on issues affecting accounts at CB&T and then refers them to local authorities to report the crime. The bank works closely with law enforcement on cases involving their customers.

CB&T is also taking steps to incorporate identity theft training into the bank's regular training program, using as one of their tools an adaptation of a brochure

Weddle developed for use in community presentations. In addition, the bank has taken steps to enhance its security policy to cover identity theft.

At Provident Bank in Baltimore, protecting customers from becoming victims of identity theft is considered "standard operating procedure." Since November, 47 cases of identity theft were documented within Provident Bank thanks to proactive initiatives by employees.

For example, Anne Benney, an 18-year veteran of Provident Bank who works as a deposit collection manager, recently added "Fraud Finder" to her title after she discovered a potential area for trouble. Benney noticed that the onset of Internet and phone/mail applications for deposit accounts meant that in some cases the bank no longer "sees" the customer and, therefore, could not check forms of identification. She decided to take a closer look at some of the Internet and phone/mail accounts that had been opened up from other states. Through credit reports and other methods, Benney found several customers whose addresses did not match the account

It Can Happen To You, Too

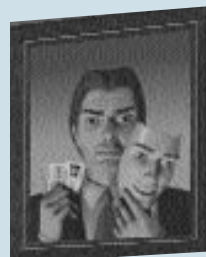
Identity theft is not a crime that simply happens to the naive; it can happen to anyone, including a very savvy compliance professional:

"Imagine my surprise at receiving a call four months ago from the MBNA security department. The security department representative asked whether I had authorized a \$1,185 purchase at a Burlington Coat Factory store. When I responded most emphatically that I had not, he asked whether I had authorized a \$10,000 cash advance at an East Coast bank. Again, I was quite sure I had not.

Just a few days before receiving that call, I had wondered why I hadn't received a bill for the \$225 in purchases on my new credit card. Given the events that followed, I have to assume that the bill was intercepted before it reached me.

Even with the card issuer's cooperation, this fraud has taken me months to straighten out. Four months after the fact, finance and late charges attributable to the fraud remained on my bill. Through the years, I have endeavored to use my own bank's products so I could look at things from the customer's perspective. While being a fraud victim probably takes this philosophy too far, I think I'll be more sympathetic next time a customer makes a fraud claim."

Kathleen Quenneville, General Counsel,
The Mechanics Bank Richmond, California



Precautionary Measures

The following list provides tips on how you — and your bank customers — can stop an ID theft before it happens. Proactive measures provide the best protection for your assets and your good name.

1. Do not give out financial information such as checking account and credit card numbers — and especially your social Security number — on the phone unless you initiate the call and know the person or organization you're dealing with.
2. Do not pre-print your driver's license, telephone, or Social Security numbers on your checks.
3. Report lost or stolen checks immediately. Also, review new checks to make sure none has been stolen in transit.
4. Store cancelled checks — and new checks — in a safe place.
5. Guard your personal identification numbers (PINs) for your ATM and credit cards, and do not write on or keep your PINs with your cards. You should also guard your ATM and credit card receipts. Thieves can use them to access your accounts.
6. Be creative in selecting personal identification numbers for your ATM and credit cards, and passwords that enable you to access other accounts. Do not use birth dates, part of your Social Security number or driver's license number, address, or children's or spouse's names. Remember: If someone has stolen your identity, he or she probably has some or all of this information.
7. If you receive financial solicitations that you're not interested in, tear them up before throwing them away, so thieves can't use them to assume your identity. Shred or make unreadable any other financial documents, such as bank statements or invoices, before disposing of them.
8. Do not put outgoing mail in or on your mailbox. Drop it into a secure, official Postal Service collection box. Thieves may use your mail to steal your identity.
9. If regular bills fail to reach you, call the company to find out why. Someone may have filed a false change-of-address notice to divert your information to his or her address.
10. If your bills include suspicious items, do not ignore them. Instead, investigate immediately to head off any possible fraud before it occurs.
11. Periodically contact the major credit reporting companies to review your file and make certain the information is correct.

For a small fee, you can obtain a copy of your credit report at any time. (Please note that in some states or municipalities, you may be legally entitled to these reports free of charge. Check with the credit bureau when ordering the report.) The three major credit bureaus and their phone numbers follow:

Equifax (800) 685-1111
Experian (800) 682-7654
TransUnion (800) 916-8800

addresses or phone numbers. The bank attempted to contact the customers by telephone or mail using the information shown on the credit reports and found several identity takeovers. As a result, employees like Benney now run credit reports on customers who open up their accounts without being seen by bank personnel.

Provident customers who have been victims of identity theft are, understandably, relieved that employees uncovered the information. One customer in Laurel, Maryland, learned that someone who gave an address in Greenbelt had assumed his identity. He also found out that the "thief" had used his identity to secure an account for a cellular phone service. He cancelled the account immediately and thanked Provident for the alert.

Expanded training programs, community seminars, close working relationships with local law enforcement, victim's kits, and focused employees are a few of the techniques financial institutions can use in the fight against this pervasive crime.

A victim in Arnold, Maryland, was notified by Provident that an account had been set up using that person's name with a California address. The victim, who is not a customer of the bank — at least not yet— said, "If this is what you do for noncustomers, I can't imagine how much you would do if I had been a real customer."

In all cases of known identity theft, Provident provides the victim with a copy of an ID theft brochure and verbal advice on the importance of securing information. Benney says it is truly a cooperative effort because many departments within the bank, such as Loss Prevention and Security, have contributed information that pointed to an

identity takeover. "I know we have increased our costs for credit reports, long distance calls, postage, etc., but our proactive efforts will keep the bank from assuming nonrecoverable losses. At the same time, we'll also help our customers guard against and recover from identity theft," Benney said.

"Banks play a significant role in prevention of ID theft with strict privacy policies and procedures," noted Dennis Algieri, senior vice president of The Washington Trust Company. "The Identity Theft Tool Kit developed by the ABA is a good resource."

The Washington Trust Company has instituted a training program on fraud prevention for employees that includes what to do if a customer claims his

or her identity has been stolen. The bank's security department is involved in this training, and the course includes information on how to handle pretext calls to prevent customer information from falling into the hands of would-be thieves.

If a customer claims identity theft, steps must be taken immediately. It is important to spend a sufficient amount of time with customers in this situation as many have never had this happen before and may be confused about the correct procedures to follow.

Washington Trust closes old accounts and opens new ones for identity theft victims. The bank also provides assis-

tance with automated clearinghouse (ACH) issues, especially Social Security checks. In addition, ID theft victims are advised to contact all credit bureaus and are given pertinent information, such as toll free numbers, for those agencies. These customers are advised to get copies of their credit reports, to let the bureaus know if they spot problems, to contact other banks and other creditors, and to contact the local police.

Chase Manhattan Bank has recognized the urgency to educate its employees, customers, and consumers in general on identity theft. In 2000 Chase launched an education and awareness campaign on the crime that includes both proactive and reactive measures. Preventive tips were given to customers of the bank in regular statement mailings and customer newsletters, and ATM messages were displayed to communicate to an even broader audience. An Identity Theft Victim Kit was created to assist victims. The kit provides the names and contact information for key agencies, including the major credit bureaus, information on other important contacts, a checklist to assist customers keep track of the contacts they have made, and samples of letters to use to begin the process of disputing charges. Along with information on dealing with the aftermath of an identity theft, Chase's kit also includes sections describing how identity theft may occur and how to protect personal information in the future. The kit is made available to any Chase customer who calls to report a case of identity theft to the bank, and Chase also provides information on its Web site.

In addition, Chase sponsored events in New York and Houston, two of the top six cities registering identity theft cases. The events were open to the public, but

had a focus for elderly and minority members of the community. Mari Frank, a leading speaker on identity theft, along with representatives from various external organizations, including the FTC, U.S. Postal Inspectors Office, America Online, Experian, the American Association of Retired Persons, and local law enforcement participated. The seminars promoted awareness and provided tips on preventing the crime, as well as what to do if identity theft is discovered.

Expanded training programs, community seminars, close working relationships with local law enforcement, victim's kits, and focused employees are a few of the techniques financial institutions can use in the fight against this pervasive crime. Whether you are in the big city or our nation's heartland, identity theft can strike indiscriminately. Many financial institutions are just realizing that what they have been investigating as fraud cases are in fact variations of identity theft. The bottom line, educating employees and customers to be aware and act immediately if they discover the crime, will go a long way toward combating this rapidly growing problem of the 21st century.

For more information about identity theft, visit the Federal Trade Commission's consumer Web site at www.consumer.gov/idtheft, or call the FTC toll-free at (877) IDTHEFT (438-4338). ❖

For more information about ABA *Bank Compliance* or to subscribe, call (800) BANKERS.

about the author

Lynne Sanders, vice president for JP Morgan Chase & Co. has been in the banking profession for more than 15 years. She has worked in the retail consumer division of the corporation her entire career, specializing in regulatory activities. In her current position in compliance and operational risk management, Sanders focuses on privacy and identity theft. She has actively worked to support legislative efforts in Washington on identity theft. Sanders has a bachelor's of science degree in business management from CWPost, LI University and a master's in finance from Pace University.

Special thanks to the following people who contributed bank and personal experiences for this article: **Kathy Steller**, vice president, JP Morgan Chase & Co.; **Thomas W. Bernoski**, vice president and compliance officer, Provident Bank; **Vicki Cox**, public relations and community relations manager, Provident Bank; **Kathleen Quenneville**, senior vice president and general counsel, The Mechanics Bank; **Barbara McGuire**, vice president, compliance, Commerce Bank & Trust; and **Dennis Algieri**, senior vice president, compliance, The Washington Trust Company.