September 15, 2002

Federal Reserve Bank of Cleveland

What You Should Know about Identity Theft

by Paul W. Bauer

Identity theft—appropriating someone else's identity for illicit gain—is the fastest-growing financial crime. It can cause considerable financial losses, and cleaning up a trashed credit history can be time consuming and frustrating. This *Economic Commentary* examines the identity theft phenomenon—how it works, how lawmakers, regulators, and financial institutions are combating it, and what consumers can do to protect themselves.

Identity theft is nothing new. It is an ancient form of fraud, intended to appropriate a person's property or lawful rights. Nor has there ever been any ambiguity about whether acquiring property by misrepresenting oneself is a criminal act. If the crime is not new and existing laws at least seem to have addressed it, why all the buzz now? The main reason is that identity theft is the fastest-growing financial crime. Since 1998, reports of Social Security number fraud have increased 500 percent. The Federal Trade Commission found that identity theft was involved in more than 40 percent of the consumer complaints it received in 2001—double what it was in 2000. Experts have attributed this crime's fast growth to the ease with which it can sometimes be committed, the high rate of return, and the low probability of getting caught.

In 2000 alone, credit card fraud caused losses of about $1 billion, a figure that underestimates the true damage because direct losses represent only about half of the cost to financial institutions. Direct losses are matched by higher expenditures for fighting the crime through technology, personnel training, legal counsel, and consumer education. These costs are expected to climb further as financial institutions step up their anti-theft efforts.

This *Economic Commentary* examines the identity theft phenomenon, detailing how it works and what lawmakers, regulators, and financial institutions are doing to combat it. More importantly, the *Commentary* discusses what you can do to protect yourself. Identity thieves have a head start, but a layered defense by law enforcement, financial institutions, and consumers, while not eradicating identity theft, can reduce its impact.

What Is Identity Theft?

Criminals have been appropriating other people's identities to perpetrate fraud for centuries, probably since civilization began. Until recently, they have been prosecuted only for the fraud committed. For example, a person discovered using someone else's identity to pass bad checks would be prosecuted only for check fraud, not for impersonation. Identity theft in itself was not explicitly outlawed until the Identity Theft and Assumption Deterrence Act of 1998. The act makes it a federal crime to "knowingly transfer or use, 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." Under the act, a "means of identification" can be a name, a Social Security, credit card, or cellular phone serial number—or any other piece of information that can be used alone or combined with other information to identify a specific person.

Because prosecutors are only required to show intent, the act allows them to pursue identity thieves even before any property has been stolen. Conviction carries a maximum penalty of 15 years in prison and possibly a fine, plus forfeiture of any personal property used or intended to be used for committing the crime. Of course, identity thieves can still be charged with violating other statutes, such as those outlawing fraud committed by means of credit cards, computers, mail, wire, financial institutions, or Social Security numbers. Some of these federal offenses carry maximum prison terms of 30 years.

Identity thieves have many ways to obtain personal information. Commonly, they steal your wallet, your purse, or maybe your mail. They might complete a change of address form to divert your mail to another location, or even rummage through your trash. Using a less intrusive approach, they might call a credit bureau, posing as a landlord, an employer, or someone else with a legitimate need for information. Alternatively, thieves might buy your personal information from an inside source at an institution that has it on file. Note that none of the techniques just mentioned involve the Internet; that territory, however, could become fertile ground for identity thieves in the coming years.

Once a thief has obtained your personal information, his next move is to cash in at your expense. One technique is to call your credit card issuer and change the

ISSN 0428-1276

mailing address. The average American household has five credit cards, so the thief might be able to run up charges on one of your accounts for some time before you realize there is a problem.

Another technique is to open a new credit card account with your name, date of birth, and Social Security number. The thief maxes out the card and you don't find out about it until the delinquent account appears on your credit report. This theme has many variations, but the object is always to gain control of your financial accounts or fraudulently apply for credit in your name to obtain goods and services.

What Can You Do to Minimize the Risk?

Just as you cannot prevent a determined burglar from breaking into your house, you cannot make your identity 100 percent secure, but you can work with financial institutions and law enforcement agencies to minimize your risk (see the "Consumer Resources" sidebar). Police and prosecutors are gaining experience in combating identity theft. The Federal Trade Commission has taken several steps to increase public information about the dangers of this crime and ways to combat it. The FTC devotes 50 to 55 full-time staff members to privacy issues and handles about 3,000 telephone reports of identity theft every week. It is working with the three major credit reference agencies to develop a system in which a single phone call puts fraud alerts on all your accounts. This should help deter identity thieves who get around fraud alerts by applying for credit in several states. Finally, the FTC has developed a standard affidavit that dozens of credit bureaus and financial institutions have agreed to accept, instead of requiring victims to fill out a separate form for each.

Financial institutions too are taking further action against identity theft. If you have ever used your credit card to buy expensive electronic equipment from two different stores in the same day, the card company has probably called to confirm that you authorized the purchases. Credit card companies have invested in sophisticated programs that flag patterns consistent with credit card fraud in order to reduce their losses by spotting violations sooner.

Congress has also been active. In addition to the 1998 identity theft act discussed earlier, the Gramm-Leach-Bliley Act (1999) requires financial institutions to establish information security programs that protect nonpublic consumer data from internal and external threats. In addition, financial institutions must give their customers the opportunity to opt out of sharing information with nonaffiliated third parties in certain circumstances. Furthermore, the act prohibits anyone from obtaining or trying to obtain customer information by making a false, fictitious, or fraudulent statement to a representative of a financial institution. A bill that is now pending would limit the information printed on credit card receipts, a practice that many merchants have already adopted voluntarily.

As an individual, you can take several steps to reduce your chances of becoming a victim. First of all, you are not obliged to give out personal information merely because someone has asked for it. Before disclosing anything, find out how your responses will be used and whether they will be shared with others. Under the consumer privacy provisions of the Gramm-Leach-Bliley Act, you may prevent financial institutions to which you have provided information from sharing it with nonaffiliated third parties. Even more important, you can shop around for a financial institution that handles your personal information as you think it should. If enough consumers take this approach, firms will be obliged to compete, not only on price and service, but also on how well they protect consumers' personal information.

You can protect yourself further by remembering how identity thieves work. Reduce the amount of junk mail you receive by calling credit bureaus and national marketing associations to request that they remove your name from preapproved offers. Before you throw away documents that contain sensitive information such as Social Security and credit card numbers, shred them. This will frustrate trash-picking identity thieves. Be alert to possible attempts at social engineering, in which a caller pretends to represent your bank and asks you to confirm some account information. Never disclose any personal information, whether by phone, mail, or Internet, unless you know who you're dealing with.

Be alert to unusual occurrences. A credit card bill that does not come on time may have been delayed or lost in the mail; but it is also possible that an identity thief has taken over your credit card account and changed your billing address to cover his tracks. Remember that these criminals still use decidedly low-tech methods to get most of the personal information they need, and you can use low-tech methods to counter them. Whenever possible, deposit outgoing mail in post office collection boxes or, better yet, at your local post office. As for incoming mail, collect it as soon as possible; to be still safer, get a post office box. If you cannot pick up your mail for a few days, have the Postal Service hold it.

Pickpockets and purse snatchers are yet another source of personal information for identity thieves, so carry only essential identification and only the credit cards you are likely to need. Slightly more sophisticated methods of thwarting identity thieves include putting passwords on your credit card, bank, and phone accounts. Be sure to choose a password you will remember, but avoid using easily available information such as your mother's maiden name, your birth date, or the last four digits of your Social Security number.

Some privacy experts advise consumers to obtain a copy of their credit report periodically to ensure that no unauthorized activity is going on under their name.

What to Do If It Happens to You

If, despite all precautions, the worst happens and you become a victim of identity theft, federal laws mandate procedures for correcting credit report and billing errors and for stopping debt collectors from dunning you for sums you do not owe. Nonetheless, the process of setting matters straight is often time consuming and frustrating for the victim.

The Truth in Lending Act limits your liability for unauthorized credit card charges to $50 per card in most cases. The Fair Credit Billing Act establishes procedures for resolving billing errors on your credit card accounts, including fraudulent charges.

If someone steals your checks and forges your signature, there are no federal statutes that limit your losses, but state laws offer some protection. Most states hold the bank responsible for

losses from a forged check—provided that you have taken reasonable care of your account and you notify the bank promptly that a check was lost or stolen.

The Fair Credit Reporting Act establishes procedures for correcting mistakes on your credit records and requires that access to your records be limited to people who have a permissible purpose. If you file a claim with a credit bureau stating that your records are inaccurate, the credit bureau must investigate it in a timely manner, usually within 30 days. It must delete from your file any disputed information that cannot be verified and must also correct erroneous information. In addition, you can have the credit bureau send notices of the corrections to anyone who received your report in the previous six months—the previous two years if the request was made for employment purposes. Finally, if the investigation does not resolve your dispute, you can write a statement about the dispute and have the credit bureau include it in your file and in future reports.

Even though the law gives you important protections and rights, the old proverb still holds: An ounce of prevention is worth a pound of cure.

Conclusion

Criminals have long benefited by misrepresenting themselves to others, but the development of modern financial markets and the vast amount of data available to the public (and increasingly accessible on the Internet) have combined to make identity theft a profitable, relatively low-risk endeavor. This white-collar crime inflicts no physical harm, but it can exact high economic costs in victims' loss of funds and their prolonged, complicated efforts to repair their credit history. As with most other crimes, direct victims are not the only ones who suffer. In the long run, all users of financial services products end up paying higher fees or interest rates to cover financial institutions' losses.

Because identity theft is perpetrated for financial gain, the way to deter it is to reduce the crime's profitability by making it harder to commit, increasing the odds of getting caught, and ensuring that the penalties are severe enough to be a deterrent. Law enforcement agencies and financial institutions have begun gearing up to fight identity theft, but they still have a long way to go.

In the evolving cat-and-mouse game between law enforcement and criminals, the balance of power is only just starting to shift toward enforcement. Consumers will need to play a significant role in deterring this crime and bringing perpetrators to justice. To protect yourself, be sure you understand the risks, take suitable precautions, and report suspicious activity to the appropriate authorities. Identity thieves are constantly expanding their bag of tricks, so be alert to any irregularity—it could be your first hint that someone is tampering with your good name.

CONSUMER RESOURCES

For more information on identity theft, see:

"When Bad Things Happen to Your Good Name," Federal Trade Commission, www/consumer.gov/idtheft. "Identity Thieves Thriving," *Bank Technology News*, April 2002, vol. 15, no. 4.

To check your credit rating, contact one of the major credit reference agencies:

Experian (formerly TRW), P.O. Box 8030, Layton, UT 84041-8030, (888) 397-3742, www.experian.com

TransUnion, P.O. Box 390, Springfield, PA 19064, (800) 916-8800, www.transunion.com

Equifax, P.O. Box 740241, Atlanta, GA 30374-0241, (800) 685-1111, www.equifax.com

To file an identity theft complaint by phone, toll free: 1-877-ID-THEFT (438-4338)

online: https://rn.ftc.gov/dod/widtpubl$.startup?Z_ORG_CODE=PU03

by mail: Identity Theft Clearinghouse, Federal Trade Commission 600 Pennsylvania Ave., NW, Washington, DC 20580

To opt out of prescreened credit card offers (the source of many identity thefts) by phone, toll free: 1-888-5-OPT-OUT

To learn about privacy choices for your personal financial information online: http://www.federalreserve.gov/pubs/privacy/default.htm

Paul W. Bauer is an economic advisor at the Federal Reserve Bank of Cleveland. *The author thanks several anonymous readers for their helpful comments.*

The views expressed here are those of the author and not necessarily those of the Federal Reserve Bank of Cleveland, the Board of Governors of the Federal Reserve System, or its staff.

Economic Commentary *is published by the Research Department of the Federal Reserve Bank of Cleveland. To receive copies or to be placed on the mailing list, e-mail your request to* 4d.subscriptions@clev.frb.org *or fax it to* 216-579-3050. Economic Commentary *is also available at the Cleveland Fed's site on the World Wide Web:* www.clev.frb.org/research, *where glossaries of terms are provided.*

We invite comments, questions, and suggestions. E-mail us at editor@clev.frb.org.

Federal Reserve Bank of Cleveland
Research Department
P.O. Box 6387
Cleveland, OH 44101

Return Service Requested:
Please send corrected mailing label to the above address.

PRSRT STD
U.S. Postage Paid
Cleveland, OH
Permit No. 385