

UNITED STATES POSTAL INSPECTION SERVICE LAW ENFORCEMENT REPORT

Mail this postcard to people and businesses that send you mail.

My Name (Last name, first name, middle initial)

OLD Address
 OLD Complete Street Address or PO Box or Rural Route and RR Box Apt./Suite #
 City or Post Office State ZIP or ZIP+4 Code

NEW Address
 NEW Complete Street Address or PO Box or Rural Route and RR Box Apt./Suite #
 City or Post Office State ZIP or ZIP+4 Code

NEW Telephone Number (Optional)

Account Number (If applicable)

Signature Today's Date: M

Identity Theft: Stealing your name and your money

Mail this postcard to people and businesses that

My Name (Last name, first name, middle initial)

OLD Address
 OLD Complete Street Address or PO Box or Rural Route and RR Box
 City or Post Office State

NEW Address
 NEW Complete Street Address or PO Box or Rural Route and RR Box
 City or Post Office State

NEW Telephone Number (Optional)

Account Number (If applicable)

Signature

In what many are calling America's fastest growing type of robbery, crooks are working without the usual tools of the trade. Forget sawed-offs and ski masks: your social security number will do the trick. Or that blank, pre-approved credit application you tossed out with the coffee grounds. Even talking on your phone could allow someone you may never meet to rob you of the one thing you may have thought safe from attack: your identity.

Mail this postcard to people

My Name (Last name, first name, middle initial)

OLD Address
 OLD Complete Street Address or PO Box or Rural Route and RR Box
 City or Post Office State

Identity fraud is digging deep into consumer's pockets — millions of dollars were lost in the past year by financial institutions across the country. The perpetrator may use a variety of tactics to drain your finances: posing as a loan officer and ordering your credit report (which lists account numbers); "shoulder surfing" at the ATM or phone booth to get your PIN code; "dumpster diving" in trash bins for unshredded credit applications, canceled checks or other bank records; or, until recently, notifying the Postal Service to redirect your mail to the address of choice, such as a mail drop, which allows anonymity.

It may be months before you're aware you're a victim. But when you get turned down for a mortgage on your dream house because you've got a bad credit rating and you know you've paid the bills, beware: the ID thief may have struck again.

on the Internet. What's worse, most states still use your SSN for your driver's license number — a policy that is, fortunately, changing.

If you think you're safe after your wallet was stolen because you canceled your credit card and put a "stop" on your checking account, think again. Once identity thieves have the information, they may open new accounts or lines of credit — under your name, for their use.

Do you carry your social security number in your wallet? Consider this: that nine-digit code gives crooks access to your medical, financial, credit and educational records. There are no legal restrictions on private company use of social security numbers (SSNs); in fact, a data base of names with associated SSNs recently was found published

I didn't have to go far to find a victim of identity fraud: a co-worker had learned about it the hard way. His bank called him in April this year and asked, "Did you authorize a \$4,500 cash advance on your credit card in Miami, FL today?"

He was stunned. The bank had called only hours after the withdrawal was made, following an alert initiated because certain account parameters indicated something might be wrong. Luckily for him, the bank simply asked that he sign an affidavit that he had not been in Miami and hadn't made the withdrawal. He wasn't held liable for the money. And he never found out what ID the crook had used to get access to his account.

Unfortunately, my co-worker's ordeal wasn't over. He received a call in June from a cellular phone company, asking if he'd opened an account with them in Miami. Someone had racked up \$1,800 in calling charges under his name, and then disappeared.

"What really disturbed me was that they asked if I lived at an address in Hallendale, FL. This guy was using my name and social security number — he was pretending to be me! He could kill someone or rob a bank with my ID in his pocket!"

Once again, he signed an affidavit disclaiming knowledge of the charges, and the account was cleared. This time, he called the three main credit bureaus and reported the fraud. He's thinking about buying a new house this year, and he's worried these incidents could mar his otherwise clean credit history.

My co-worker is just one of thousands of individuals who are victimized each year. The July 1995 edition of *Kiplinger's Personal Finance Magazine* reported that Experian (TRW), one of the three largest credit bureaus, was getting 600 to 700 new fraud cases every day, and more recent tallies show those figures are still on the rise. The culprits may be found among employees (or patrons)

of mailrooms, airlines, hotels or personnel offices — anyone who has access to a person's financial information.

They can use your credit card or instead use encoding equipment, sold by business supply companies, and blank cards with magnetic strips on the back, to encode your account number onto a counterfeit card with a different name. Crooks sometimes seek jobs specifically to get access to financial information; alternately, they may bribe employees in such positions to supply them with the data they want.

Need a phony ID to "prove" you're the person whose name is on the credit card? Try surfing the Web. There are scores of sites with complete instructions on creating a "new you." And if you've got your own computer, "scanner" and color printer (or copier), you can create your own false documents.

In a typical case in the first half of this year, Postal Inspectors arrested eight West African nationals who were allegedly operating a multimillion dollar counterfeit and stolen credit card enterprise nationwide. And Postal Inspectors in New York arrested 16 members of a gang that allegedly ran

a passport photo business, supplying false identifications for cashing checks stolen from the mail.

Securing Your Finances

- If you think you're a victim of fraud, call your credit card issuers to close or "flag" your accounts, and call your bank to put an alert on your checking accounts.
- Empty your wallet of extra credit cards (and IDs) — or better yet, cancel the ones you don't really use and keep a list of the ones you do use.
- Never give out personal information over the phone, such as your date of birth, mother's maiden name, credit card number, social security number or bank PIN code, except to someone you know or an established firm.
- Shred pre-approved credit applications, credit card receipts, bills and other financial information you don't want before tossing them in the trash.
- Financial institutions or businesses that handle personal information should protect customers' privacy by storing such material securely and ensuring it has limited access. It is essential to shred such material before disposing of it.
- Consider removing your name from the marketing lists of the three major credit reporting bureaus: Experian at 800-353-0809, Equifax at 800-219-1251 and TransUnion at 800-241-2858. This reduces the number of pre-approved applications you receive in the mail.
- Order your credit report once a year to check for accuracy or fraudulent use.

In response to recommendations by the Chief Postal Inspector of the Postal Service, a recent prevention measure that addresses some of consumers' concerns was adopted by the U.S. Postal Service. Aware that a crook could submit an address change to divert customers' mail without their knowledge, post offices now send a "Move Validation Letter" to both the old and new address when a change is filed. The letter requests you call an "800" number if you did not file the change.

Postal Inspectors have jurisdiction to investigate and enforce over 200 federal statutes involving the U.S.

Mail. Under Title 18, U.S. Code, Section 1708, they may arrest individuals suspected of stealing mail or filing a fake change of address; the penalty is a \$2,000 fine or up to five years' imprisonment, or both. If someone applies for a credit card in your name, they may be prosecuted under Title 18, USC 1341; the penalty is a \$1,000 fine or up to five years' imprisonment, or both — unless a financial institution is affected, in which case the fine may be raised to \$1 million and imprisonment for up to 30 years.

Other preventive steps are being taken to combat ID theft: the card activation system (an idea proposed by a Postal Inspector), which requires

that credit card owners call the issuer upon receipt to ensure the cards are in the right hands; credit checks, in which creditors check card applications against various fraud data bases before issuing a new card; and new methods of encoding the magnetic strip on credit cards to increase their security.

But don't depend on these measures for your peace of mind. Read the information in the boxes on these two pages to protect yourself from those that prey on your money. And your name. ■

Who to Call for Help

- Report credit card fraud to the three major credit reporting bureaus: Experian at 800-301-7195, Equifax at 800-525-6285 and TransUnion at 800-680-7289.
- If you've had checks stolen or bank accounts set up fraudulently in your name, call these check guarantee companies: Telecheck at 800-366-2425; and the National Processing Company at 800-526-5380. They can flag your file so that counterfeit checks will be refused.
- If your social security number was used fraudulently, report the problem to the Social Security Administration's Fraud Hotline at 800-269-0271. In extreme cases of fraud, it may be possible for you to get a new SSN.
- If fraudulent charges appear on your account, call the Consumer Credit Counseling Service at 800-388-2227 for help in clearing false claims from your credit report.
- If you're a victim of identity theft that involves the U.S. Mail, call your nearest Postal Inspection Service office, listed in the back of this publication, and your local police.

This article was written by Debbi Baer, Congressional & Public Affairs, National Headquarters, with special thanks to Postal Inspector Henry Herrera, Philadelphia Division, and Postal Inspector John Scott, Program Manager, Criminal Investigations, National Headquarters. For more information on fraud schemes that involve the U.S. Mail, visit our website at www.usps.gov/websites/depart/inspect.