

## IDENTITY THEFT BOOMING

This rather broad topic takes in any number of privacy crimes, including theft of a Social Security number, a credit or debit card, or even the pilfering of phone calling cards.

The numbers associated with identity theft are beginning to add up fast. A recent General Accounting Office report estimates that as many as 750,000 Americans are victims of identity theft every year. And that number may be low, as many people choose not to report the crime or for that matter, even know they've been victimized.

### How it can happen:

Officials say much of Identity Theft still comes down to hands-on mischief – things like 'Dumpster diving', and 'shoulder surfing'. Officials also acknowledge that the Internet has opened new avenues for theft. If nothing else, the Web allows thieves to send stolen data to most any worldwide location.

One popular scam involves fake mortgage brokers and still another uses e-mail in which the sender poses as an Internet service provider asking for information.

Then, as if the cost of some restaurant meals isn't unsettling enough, there's the infamous "skimmer".

"A skimmer is about the size of a credit card. "And a criminal buys off a waiter in a restaurant. When you give him your credit card, he rings it up but also runs it through the skimmer, which collects your credit card information. In exchange for \$50 a card, a waiter can gather as many as 100 credit cards a night."

A Social Security card can also reap long-term fraudulent benefits. Virgil Gardaya, a corporate vice president with the credit bureau Equifax, notes that a stolen wallet containing a Social Security card lets a criminal quickly set up dummy bank and savings accounts. The very

presence of the account may prompt the bank to give the criminal a credit card. From there, the con artist may waste little time maxing out the card, or take a bit more time and build up the card's buying power. That can mean fraudulent purchases as pricey as cars and boats.

## SIMPLE WAYS TO PROTECT YOURSELF

There's no ironclad protection that guarantees that you'll never fall victim to some form of identity theft. But there are steps you can take to shield your privacy.

- Destroy private records and statements.
- Empty your mailbox quickly so criminals don't have a chance to snatch credit card pitches, lock your mailbox.
- Don't carry your Social Security card with you, or any card that may have your number. Don't put your number on your checks. Leave your driver's license number off your checks as well.
- Never leave ATM or gas station receipts behind.
- Worried about credit card skimming? Pay with cash as often as possible.
- When making an online purchase, look in the lower right hand corner of your browser window. If you see the icon of a lock, that means you're dealing with a secure site. If you don't see one, you'll be safer finding another merchant.
- Stick to well-known retailers or sites that others have used to their satisfaction. Use only one credit card for online purchases. That way, if something amiss happens, it'll be easier to spot on your bill.
- Be more defensive with personal information. Ask salespeople and others if information such as a Social Security number or driver's license is absolutely necessary. Ask anyone who requires your Social Security number—for instance, your insurance company what their privacy policy is and whether you

can arrange for the organization not to share that information with anyone else.

- Check your credit report at least once a year to look for suspicious activity. If you spot something alert your card company or the creditor immediately.
- Investigate credit bureau protection services. For instance, Equifax offers Credit Watch.

## IF SOMETHING GOES WRONG

Again, protecting yourself from security fraud is no sure thing. But there is plenty you can do if you uncover some wrongdoing.

- First, contact the fraud department of each of the three major credit bureaus. Tell them that you're an identity theft victim. Request that a "fraud alert" be placed in your file, along with a victim's statement asking that creditors call you before opening any new accounts or changing your existing accounts.

### Equifax

To order a report: 1-800-685-1111

Or write: P.O. Box 740241, Atlanta, GA 30374-0241

To report fraud: 1-800-525-6285 and write: P.O. Box 740241, Atlanta, GA 30374-0241

### Experian

To order a report: 1-888-EXPERIAN (397-3742) or write: P.O. Box 2104, Allen, TX 75013

To report fraud: 1-888-EXPERIAN (397-3742) and write: P.O. Box 9532, Allen, TX 75013

### TransUnion Set up an e-mail garbage address. Use one e-mail address for transactions and other activities

To order a report: 800-916-8800

Or write: P.O. Box 1000, Chester, PA 19022

To report fraud: 1-800-680-7289 and write:

Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92634

- Contact the creditors for any accounts that have been tampered with or opened

fraudulently. Speak with someone in the security or fraud department of each creditor and follow up with a letter.

- File a report with your local police or the police in the community where the identity theft took place. Get a copy of the police report in case the bank, Credit-card company or others need proof of the crime.
- Keep records of everything involved in your efforts to clear up fraud, including copies of written correspondence and records of telephone calls.

### **De- spamming yourself**

Whether a mere annoyance of a lucrative venue for thieves, solicitations via phone, mail or the internet may seem an inescapable element of modern life. But like other privacy issues, there are steps you can take to mitigate the problem.

- First, the Direct Marketing Association maintains a service through which consumers can remove themselves from mail, phone and e-mail solicitation lists. Here's the drill:
- To get off the mail list, write to Mail Preference Service, Direct Marketing Association, P.O. Box 9008, Farmingdale, NY 11735. When giving your name, use full names, nicknames and any other combination that a solicitor may use.
- To get off the phone list, send your name, address and phone number to Telephone Preference Service, DMA, Box 9014, Farmingdale, NY 11735. Make sure you provide all phone numbers you may use.

### **You also might want to try these tips:**

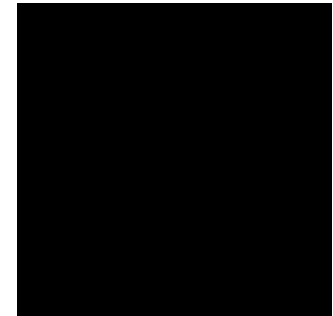
- If you get an unwanted e-mail, don't click the "remove me" option, all that

means is that the mail has hit an active address.

- Set up an e-mail garbage address. Use one e-mail address for transactions and activities that may lead to spams. Use another for all private communication.
- Besieged by telephone solicitations? Just tell them not to call again. The Telephone Consumer Protection Act of 1991 stipulates that they have to do so if you ask.
- Contact your card company and find out how to take part in their "opt out" program. This prevents your name from being passed around to other companies you cardholder deals with.

CRIME COMMISSION  
2121 South Columbia, LL # 8  
TULSA, OK 74114  
(918) 585-5209 (FAX) 585-1015

WEBSITE ADDRESS:  
[www.crimecomok.org](http://www.crimecomok.org)



## **Identity Theft**

## **Crime Commission**

*Working with citizens for  
a safer  
Community*

*since 1971*