How You Can Thwart ID Thieves

By Jane Black

Here are several simple precautions everyone really needs to take. Ignore them at your peril

Your identity is arguably your most valuable possession. A clean legal record and credit history open the door to everything from getting a job to securing a home loan and all the other, day-to-day privileges most folks for granted. Stains on those records can take years to erase, but people tend to pay more attention to securing their cars than protecting personal data. That's why identity theft struck 9.9 million Americans last year, costing businesses and individuals $53 billion, according to a survey commissioned by the Federal Trade Commission (FTC).

On Dec. 4, President George W. Bush signed legislation to give consumers new ways to protect their identities. Among the provisions in the Fair & Accurate Credit Transactions Act: Credit-card companies and credit bureaus are required to participate in a national ID-theft alert system, financial institutions must develop a system for identifying ID theft faster and minimizing the damage before a consumer is aware of the problem, and merchants will have to black out Social Security numbers, credit-card numbers, and debit-card numbers on receipts.

While the new law may help consumers, identity thieves are a lot like car thieves, experts say: If they want something badly enough, they'll probably find a way to take it. On the other hand, if you make the thieves' job harder, they'll be more likely to search for another, easier target. Here are some simple steps you can take to protect your identity and be a less attractive target.

• **Buy a shredder.** This is one of the easiest ways to guard against "dumpster diving," says Naomi Lefkovitz, an attorney for the FTC's identity-theft program. Identity thieves prowl public dumps and big trash bins looking for credit-card statements and other sensitive documents. Many of those papers contain all the information a thief needs to hijack your identity.

• **Don't trust your e-mail.** The latest ploy of ID thieves is to send official-looking e-mail messages that appear to come from companies you've done business with. The e-mail messages request passwords and other personal data. The practice -- called "phishing" -- can dupe even savvy consumers. When in doubt, verify by phone or through the company's Web site that the e-mail and any request for information are genuine.

• **Get your credit report.** It's always a good time to get copies of your credit report from the three major credit bureaus -- Equifax, Experian, and TransUnion. It won't protect you from theft, but it will let you spot suspicious activity taking place in your name. The regular charge is around $10 for a copy, and consumers are encouraged to obtain reports from all three bureaus. Some deals offer reports from all three bureaus for a single price.

• **Protect your Social Security number.** This has become a de facto customer ID, but most of

the time, you don't have to give it away. SSNs are like spun gold to identity thieves. The FTC's Lefkovitz advises consumers to ask companies that request an SSN why they need it. Retail stores, utility companies, and insurers are among the sorts of companies that probably don't need your Social Security number -- even if they ask for it. The law doesn't prevent them from asking, but many will back down if you insist on keeping your number private.

• **Make sure your SSN isn't on your driver's license.** State motor vehicle departments are required to collect Social Security numbers before they issue driver's licenses or ID cards, but states are not required to display the number on the actual license. In most states you can ask to be issued a unique license number. A new Virginia law bans the practice of using Social Security numbers on licenses or ID cards. Maryland licenses don't use SSNs, and Washington (D.C.) residents are issued a random driver's license number unless they request otherwise.

• **Keep your mother's maiden name between you and her.** When a company asks for your mother's maiden name, what they really want is a password that only you know. Since your mother's maiden name is easily discovered, consider a different password.

• **Talk to your boss.** Some of the biggest sources of personal data are companies that fail to destroy sensitive documents or leave their computer systems unprotected. Ask your boss or human resources department how they protect your information. Some states have laws requiring safe disposal of employee documents.

• **Practice safe computing.** It's vitally important to inoculate your home computer against attacks and spying, especially if you trade music or other digital files online. Buy antivirus software and keep it updated with the latest virus definitions. Also consider firewall software.

If you're victimized:

• **Contact the three big credit bureaus.** They can place a fraud alert on your account and request that creditors call you before opening new accounts in your name. Ask for credit reports so you can track the abuse.

• **Close or suspend compromised accounts.** Contact your credit-card company and bank to report your ATM or credit card stolen. Have your bank stop payment on stolen checks and contact their check-verification companies.

• **File a police report detailing the fraud.** Provide authorities with as much documentation as possible - and be persistent. Some credit bureaus will block fraudulent accounts on your card only if you have filed a police report.

• **Complain to the FTC.** It maintains a database of ID-theft cases for federal investigators.

No matter how many safeguards against theft appear to be in place, always be vigilant about protecting your identity. Don't get a false sense of security because receipts will no longer have sensitive information on them or because big institutions now are required to do more on your behalf. The stains that can blot a record for years take only minutes to form.