

Snapshot

A Focused Look at Today's Human Resource Issues

brought to you by

MARQUEE Staffing



IDENTITY THEFT The Crime of the New Millenium

The airwaves are filled with clever commercials from banking institutions which portray this devastating crime in a humorous way. For those who have been unwitting victims this crime is anything but funny.

The 1990's spawned a new variety of crooks called identity thieves. Your everyday transactions, which usually reveal bits of your personal information: your bank and credit card account numbers; your income; your Social Security number (SSN); or your name, address, and phone numbers are their stock in trade. An identity thief obtains some piece of your sensitive information and uses it without your knowledge to commit fraud or theft.

Identity theft is a serious crime. People whose identities have been stolen can spend months or years — and their hard-earned money — cleaning up the mess the thieves have made of their good name and credit record. Some victims have lost job opportunities, been refused loans for education, housing or cars, or even been arrested for crimes they didn't commit.

Many people do not realize how easily criminals can obtain our personal data without having to break into our homes. In public places, for example, criminals may engage in "shoulder surfing" - watching you from a nearby location as you punch in your telephone calling card number or credit card number - or listen in on your conversation if you give your credit-card number over the telephone to a hotel or rental car company.

Even the area near your home or office may not be secure. Some criminals engage in "dumpster diving" - going through your garbage cans or a communal dumpster or trash bin — to obtain copies of your checks, credit card or bank statements, or other records that typically bear your name, address, and even your telephone number. These types of records make it easier for criminals to get control over accounts in your name and assume your identity.

The FTC commission describes precautions which can be taken in their brochure "ID Theft: What's it all about".

Can you prevent identity theft from occurring?

As with any crime, you cannot completely control whether you will become a victim. But, according to the Federal Trade Commission (FTC), you can minimize your risk by managing your personal information cautiously and with heightened sensitivity. Perhaps the most critical piece of information to protect is your Social Security Number.

In 2004, California legislation became effective which limits the use of your social security number as a method of identification on things such as employment applications and medical plans. As a matter of course employment applications may not ask for social security numbers as a means of identification during the initial application process. That information can be obtained at the point of hiring through the use of other forms such as the W4, I9 or background screening documents.

How can I tell if I'm a victim of identity theft?

Monitor the balances of your financial accounts. Look for unexplained charges or withdrawals. Other indications of identity theft can be:

- failing to receive bills or other mail signaling an address change by the identity thief;
- receiving credit cards for which you did not apply;
- denial of credit for no apparent reason; or
- receiving calls from debt collectors or companies about merchandise or services you didn't buy.

Are There Any Other Steps I Can Take?

- If an identity thief is opening new credit accounts in your name, these accounts are likely to show up on your credit report. You can find out by ordering a copy of your credit report from any of three major credit bureaus.
- When it involves your personal information, exercise caution. Place passwords on your credit card, bank and phone accounts. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your SSN or your phone number, or a series of consecutive numbers.
- Secure personal information in your home, especially if you have roommates, employ outside help, or are having service work done in your home.
- Ask about information security procedures in your workplace. Find out who has access to your personal information and verify that your records are kept in a secure location. Ask about the disposal procedures for those records as well.
- Don't give out personal information on the phone, through the mail, or over the Internet unless you've initiated the contact or are sure you know who you're dealing with. Identity thieves can be skilled liars, and may pose as authorized representatives. Before you divulge any personal information, confirm that you're dealing with a legitimate representative of a legitimate organization. Double check by calling customer service using the number on your account statement or in the telephone book.
- Guard your mail and trash from theft. Deposit outgoing mail in post office collection boxes or at your local post office instead of an unsecured mailbox. Remove mail from your mailbox promptly. If you're planning to be away from home and can't pick up your mail, call the U.S. Postal Service at 1-800-275-8777 to ask for a vacation hold.
- To thwart a thief who may pick through your trash or recycling bins, tear or shred your charge receipts, copies of credit applications or offers, insurance forms, physician statements, checks and bank statements, and expired charge cards.
- Keep your Social Security card in a secure place and give your SSN only when absolutely necessary. Ask to use other types of identifiers when possible. Limit the identification information and the number of credit and debit cards that you carry to what you'll actually need.
- Keep your purse or wallet in a safe place at work.

If Your Identity's Been Stolen:

Even if you've been very careful about keeping your personal information to yourself, an identity thief can strike. If you suspect that your personal information has been used to commit fraud or theft, **take the following four steps right away**. Remember to follow up all calls in writing; send your letter by certified mail, return receipt requested, so you can document what the company received and when; and keep copies for your files.

1. Place a fraud alert on your credit reports and review your credit reports.

Equifax

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

Experian

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

TransUnion

To report fraud, call: 1-800-680-7289, and write: Fraud Victim Assistance Division, P.O. Box 6790, Fullerton, CA 92834-6790

2. Contact all creditors with whom your name or identifying data have been fraudulently used.

Contact all financial institutions where you have accounts that an identity thief has taken over or that have been created in your name but without your knowledge.

Contact the major check verification companies if you have had checks stolen or bank accounts set up by an identity thief. In particular, if you know that a particular merchant has received a check stolen from you, contact the verification company that the merchant uses:

For new unauthorized accounts, ask if the company accepts the ID Theft Affidavit (available at www.ftc.gov/bcp/online/pubs/credit/affidavit.pdf). If they don't, ask the representative to send you the company's fraud dispute forms.

For your existing accounts, ask the representative to send you the company's fraud dispute forms.

3. File a report with your local police or the police in the community where the identity theft took place.

Keep a copy of the report. You may need it to validate your claims to creditors. If you can't get a copy, at least get the report number.

4. File a complaint with the FTC.

By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials track down identity thieves and stop them. The FTC also can refer victim complaints to other appropriate government agencies and companies for further action. The FTC enters the information you provide into our secure database.

To file a complaint or to learn more about the FTC's Privacy Policy, visit www.consumer.gov/idtheft.



MARQUEE Staffing HR Library

Snapshot is a publication of MARQUEE Staffing. More information about these and other issues confronting California employers is available online at www.omniexpress.com/hr_library.

This publication is for informational purposes only. Please consult with appropriate legal counsel when making policy decisions for your company.