Identity theft—who's been in your wallet?

The Federal Trade Commission estimates nine million Americans have their identities stolen every year. Identity theft occurs when an unauthorized person uses your personal identifying information, such as your name, Social Security number, credit-card number or financial account information, without permission. The most alarming aspect of this crime is that you may not realize you are a victim until reviewing your financial statements, or worse yet, you are contacted by a debt collector.

Identity theft has serious implications, such as:

- loss of money and time spent to repair damage to your name and credit record;
- loss of job opportunities;
- denied loans for housing, cars or education; and
- possible arrest for crimes you did not commit.

How does it happen?

Headlines citing this crime appear often. How are thieves accessing confidential information? Identity theft happens when thieves:

- obtain bills or other paperwork with your personal information such as bank or credit-card statements, pre-approved credit offers, new checks or tax information from your trash or mailbox;
- use special storage devices when processing your credit, debit or ATM card or break into merchants' credit-card electronic databases;
- unprotected information sent on a laptop or smartphone while using Wi-Fi;
- trick you into revealing your personal information through spam (unsolicited emails) or pop-up messages, known as phishing;
- contact you claiming they are someone else (i.e., research firm) and obtain your personal information under false pretenses;
- pose as a landlord, employer or someone else who may have a legal right to your credit report;
- divert your billing statements to another location by submitting a change of address with the firm;
- steal wallets and purses;
- steal personnel records from employers or bribe employees who have access to them; or
- listen in on phone conversations in which you provide your credit-card number.

How do I avoid becoming a victim?

So, what can you do about it? Reduce the risk and protect yourself by employing these measures:

- Shred all documents with personal information, including pre-approved credit offers, before discarding.
- Review financial account and billing statements closely for charges you did not make.
- Deposit mail in U.S. Postal Service collection boxes and never leave mail in your mailbox overnight or on weekends.
- Use fire walls, anti-spyware and anti-virus software and keep it updated.
- Do not respond to spam, pop-ups or unsolicited emails; go directly to the trusted website and make sure it is full encrypted before providing personal and financial information.
- Do not use personal identifying information for passwords, such as a birth date, mother's maiden name, Social Security number or phone number.
- Never provide personal information over the phone, through the mail or Internet unless you know the firm or person.
- Never carry your Social Security card in your wallet or write your number on a check.
- Annually, obtain your free credit report from each of the three major credit bureaus by calling (877) 322-8228 or going to www.annualcreditreport.com. Do not go directly to the bureaus, as they will charge you. Also, request each of the three bureau reports at different times to monitor your information throughout the year.
- If you are an active-duty military member and away from your usual duty station, place an active-duty alert on your credit reports to minimize the risk while deployed. This will remove your information for prescreened credit-card offers for two years.

(continued on back)

- Be careful when responding to promotions. Identity thieves can use promotional offers to get your personal information.
- If you prefer not to receive prescreened credit and insurance offers by mail, you can opt out for five years or permanently by calling toll-free 1-888-5-OPTOUT (1-888-567-8688) or visiting www.optoutprescreen.com.
- Don't buy credit card "loss protection" insurance—according to the FTC, your liability for unauthorized charges is limited to $50. Telephone scam artists will often use this pitch.
- Carry identity-theft insurance. This coverage can provide reimbursement for expenses resulting from the crime, such as phone bills, lost wages, notary and certified-mailing costs and attorney fees. It is inexpensive and may be endorsed to your homeowners or renters insurance policies. As your agent, we can provide more details on this coverage.

What should I do if I think someone stole my identity?

The federal government and many states have enacted laws against identity theft.

The FTC has a section of their website (www.ftc.gov/idtheft) which offers sample letters to law-enforcement agencies; allows the ability to request information about fraudulent transaction(s) to dispute a charge; offers a form to record the steps you've taken; and more.

Take the following steps right away to prevent further damage:

1 Put a fraud alert on all credit files. Contact only **one** of the three major credit bureaus (see *Helpful contact information* section at right), which automatically will alert the others.

There are two different alerts that may be used:

- **Initial fraud alert—**use when you think you may be a victim but not sure; protects your credit records for at least 90 days and entitles you to one free copy of your credit report from each of the three credit bureaus.
- **Extended fraud alert—**use when you know your identity has been stolen. This alert requires an identity-theft report that will remain on credit records for seven years. It also entitles you to two copies of your credit report, one right away and the other within 12 months.

Also order copies of your credit reports and review them carefully.

2. File an IdentityTheft Affidavit with the FTC (see the *Helpful contact information* section) to help authorities with investigations across the country.
3. Report the crime to your local police in person and file a police report, which may be necessary to block fraudulent information on your credit reports.
4. Contact your bank or financial firm and speak with the security or fraud department. Follow their instructions and, if necessary, close the affected account(s).
5. Respond immediately to any debt collector in writing. Keep detailed records on all your conversations and copy all pertinent correspondence.
6. If you are interested in obtaining identity-theft coverage, contact our agency for additional information.

Helpful contact information

The three major credit bureaus:

- Equifax: (800) 525-6285 or www.equifax.com
- Experian: (888) 397-3742 or www.experian.com
- TransUnion: (800) 680-7289 or www.transunion.com

- FTC Identity Theft Hot Line: (877) 438-4338 or www.ftc.gov/idtheft
- Social Security Administration: (800) 269-0271 or www.ssa.gov