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 cri did not commit.

How does it happe

Headlin crime app
How ccessing confi
inf ion? Ident appe
w ieves
- er pa k with yo
p ormation s bank o
credit-card st ment pproved credit offers, new nformation from your trash
- use special storage d ces when processing your cr t, debit or ATM card or break into merchants' credit-card electronic databases;
- access unprotected information sent on a laptop or smartphone while using publi Wi-Fi;
- trick you into revealing your personal information through spam (u ited emails) or pop-up messag as phishing;
- contact you claim are som else (i.e., resear obta your personal info false pr
- pos employ e else gal rig credit
- ert yo g s to another by tting e of address
- wall ;
- onnel records from employers o loyees who have access to them
- in on one conversations in which 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 mai collection boxes mail in your mailbox overn weekends.
- Use fire walls yware and anti-virus ware a updated.
- to spam, pop-ups or mails; go directly to the t ebsite and make sure it is full encr ted before providing personal and financial information.
- Limit the amount of personal information on social-networking sites.
- Use strong and different passwords on each online credit and banking account.
- 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.
- Destroy labels on prescription bottles before you throw them out.
- Don't share your health plan information with anyone who offers free health services.

(continued on back)

SAMPLE
©PIA Management Services Inc.

- 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.
- 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, yo[illegible] can opt out for five years or permanently by calling toll-free 1-888-5-OPTOUT (1-888-567-8688) or visiti[illegible] www. optoutprescreen.com.
- Carry identity-theft in[illegible] coverage can provide re[illegible]ment for expenses resulting fro[illegible]ime, such as phone bills, lost wa[illegible] and ce[illegible]ing costs a[illegible] fee[illegible]nsive and may [illegible]rsed t[illegible] homeown[illegible]nters[illegible]e [illegible]es. As [illegible] p[illegible]

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.consumer.ftc.gov/) which offers sample letters to law-enforcement age[illegible] allows the ability to request information about fraudulent transaction(s) [illegible]te a charge; offers a form to r[illegible] you've taken; and more[illegible]

Take the following [illegible]t away to prevent further [illegible]

1. Put a fra[illegible]t on an[illegible]ontact only [illegible]ree ma[illegible]eaus (see[illegible]*formati*[illegible] right)[illegible]lly wil[illegible] others.

   [illegible]are tw[illegible]rent [illegible] may [illegible]

   Initi[illegible]-use when you [illegible]k you[illegible]ctim but not sure; [illegible] your c[illegible]t records for at least [illegible]d entitles you to one free copy of y[illegible]t report from each of the three c[illegible]dit bureaus.

   [illegible]**ended 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. You are entitled to a free report from each credit-reporting company since you placed an initial fraud alert.

2. File an [illegible]heft A[illegible]with the FTC[illegible]*Helpful*[illegible]*information* secti[illegible]s with investig[illegible]e count[illegible]
3. Report the c[illegible]e in person and file a[illegible]hich may be necessary t[illegible]udulent information on [illegible]r c[illegible]t reports.
4. [illegible]ntact yo[illegible] financial firm [illegible]e security or fraud [illegible]ollow their instructions and, [illegible] close the affected account(s).
5. Resp[illegible]d 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
- Social Security Administration: (800) 269-0271 or www.ssa.gov

SAMPLE
©PIA Management Services Inc.