How to prevent identity theft TAKE CHARGE

Picture this: You're sitting at the kitchen table, pouring over your budget and bills, when you open your credit card bill to discover a $1200 charge you're certain you never authorized. Someone's taken your name and used it for their own purposes. You've been a victim of a growing crime and you didn't know it until now.

What is identity theft?

Identity theft occurs when someone uses your personal information without your permission to commit fraud or other crimes.

How do I avoid it?

According to the Federal Trade Commission (FTC), as many as 9 million Americans have their identities stolen each year. While it's not always preventable, there are things you can do to help keep the odds in your favor.

- Upon receiving your credit card and bank statements each month, take a close look to make sure that no unauthorized activities occurred.
- Call your bank or credit card company if a statement is late. A missing bill could be an indication that identity theft has occurred or a thief has recently obtained your information.
- Never give out personal information over email, the Internet or the phone unless you have initiated the contact. Identity thieves often pose as government officials, representatives from the bank, credit card companies or Internet service providers in order to con you into revealing your personal information.
- Use intricate passwords for your computer, email and Internet accounts. The best passwords use a combination of numbers, capital and lowercase letters. Never use something that can be easily guessed, like your maiden name, phone number or birth date, as a password.
- Shred documents, like credit card receipts and insurance forms, that show your personal information before you dispose of them.
- Don't leave outgoing mail in your own mailbox. It's incredibly easy for identity thieves to target mailboxes and pull bank numbers from checks, sensitive information from bills and a variety of other sensitive information. Instead, deposit mail directly into post office boxes.
- Cancel credit cards that you don't need or use. When canceling, tell the lender to make a note that the "card was cancelled at the cardholder's request."
- Keep your Social Security card in a safe location—never keep it in your wallet or carry it around with you. Likewise, carry only the necessary ID and credit cards with you.
- Only give out your Social Security number when it's absolutely necessary. Ask if you can use a different form of identification instead.

How do I recognize it?

Your best defense is to be aware. When it comes to your financial information, stay alert and watch for these common signs of identity theft:

1. Bills arrive for a credit card account that you never opened
2. Your credit card bills include charges you didn't make
3. Be aware of late credit card statements that arrive after the payment due date
4. Your bank statements contain unfamiliar transfers or withdrawals
5. You've ordered new checks, but they haven't arrived at your house
6. Lenders deny your requests for credit despite previously having good standing

Preventative Measures

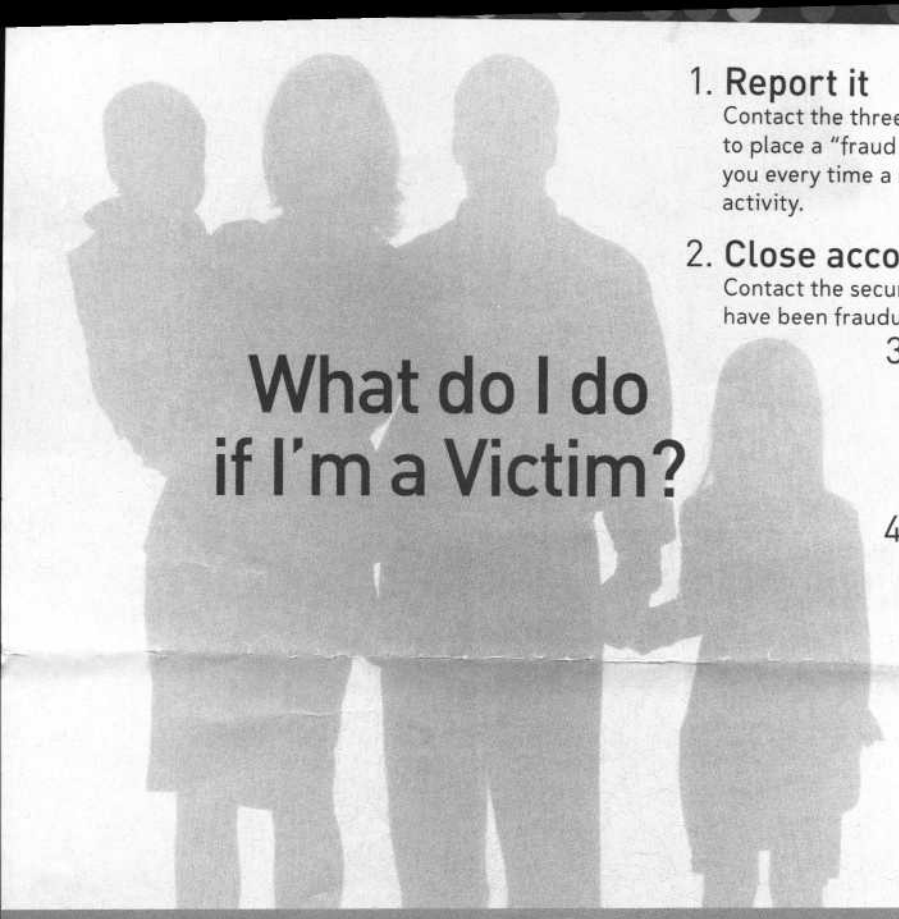
Here are several simple ways to combat the most common form of online identity theft:

- Turn on the spam filters for your email inbox. This will help identify misleading emails attempting to "phish" for your password. Be suspicious of any email that asks you to respond with personal or account information.
- Beware of scams by thieves posing as prominent companies. Double-check email addresses and website locations. Many times they have key words in them but otherwise appear unofficial, e.g. ebay2@yahoo.com.
- Use PayPal when available. Companies like PayPal are strictly regulated and are accepted around the world. Utilize their services rather than credit cards to make purchases at web sites you are unsure of.





© 2007 Buffini & Company All Rights Reserved. Used by Permission. AUGUST CAP'S



What do I do if I'm a Victim?

1. Report it

Contact the three major credit bureaus, listed on the form below, and ask them to place a "fraud alert" on your file. Some services, such as Life Lock, will contact you every time a new line of credit is requested to prevent unauthorized account activity.

2. Close accounts

Contact the security departments of the creditors or financial institutions that have been fraudulently accessed or opened.

3. Call the police

File a report with your local police and the police where the fraud took place. Get a copy of the police report so that you can submit it to your bank or credit card company if they request proof of the crime.

4. Provide details

File a complaint with the FTC. They maintain a database of identity theft cases used by law enforcement agencies for investigations. Your complaint will also help the FTC learn more about identity theft and the problems that victims experience, which will help them better assist people in the future.

After following the procedures above, keep an eye on your accounts to watch for future misuse. Change your routines to eliminate the security leak.

Chart Your Course of Action

Use the form below to record the steps you've taken to report identity theft. Document each phone call you make and letter you write, so that you have a backup if it's needed in the future.

NATIONWIDE CONSUMER REPORTING COMPANIES

Company & Contact info	Date contacted	Contact person	Comments
Equifax 1-800-525-6285 www.equifax.com P.O. Box 740241 Atlanta, GA 30374-0241			
Experian 1-888-397-3742 www.experian.com P.O Box 2104 Allen, TX 75013			
TransUnion 1-800-680-7289 www.transunion.com P.O. Box 2000 Chester, PA 19022-2000			