AVOIDING IDENTITY THEFT
IN THE AGE OF INFORMATION COMPROMISE

prevention tips to share with your friends and family

HOW DO I KNOW IF I'M A VICTIM OF IDENTITY THEFT?

Many of us have gotten a notice saying our information has been stolen. But that doesn't mean you are also an identity theft victim. A criminal has to use your information for you to be an identity theft victim. This difference is important because (1) this guide is about avoiding identity theft, not resolving it (2) you may hear about other tools that are only available to identity theft victims, and as such call for proof of the theft, sometimes in the form of a police report.

SIGNS YOU MIGHT BE A VICTIM OF IDENTIFY THEFT

Financial Accounts

- You see withdrawals from your bank account that you can't explain.
- You don't get your bills or other mail.
- Debt collectors call you about debts that aren't yours.
- You find unfamiliar accounts or charges on your credit report.

Other Benefits

- Medical providers bill you for services you didn't use.
- Your health plan rejects your legitimate medical claim because the records show you've reached your benefits limit.
- A health plan won't cover you because your medical records show a condition you don't have.
- The IRS notifies you that more than one tax return was filed in your name, or that you have income from an employer you don't work for.
- You get notice that your information was compromised by a data breach at a company where you do business or have an account.

IDENTITY THIEVES CAN USE YOUR INFORMATION ANYWAY YOU DO

Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief can file a tax return in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest.

WHY DO I NEED TO DO ANYTHING?

You are the best line of defense. Being active can save you lots of time and effort if someone does use your information. Action steps to avoid identity theft are on the next page. Contact our ID Theft Unit for additional help.

South Carolina Department of Consumer Affairs
2221 Devine St. STE 200 • PO Box 5757 • Columbia, SC 29250
800-922-1594 • www.consumer.sc.gov

ACTION STEPS
TAKE THESE STEPS TO AVOID IDENTITY THEFT:

BASIC TOOLS

Consider a security freeze. A security freeze stops anyone from looking at your credit report, unless you lift it. It stops criminals from opening up new accounts using your information. The freeze does not affect your existing accounts, so you will need to monitor your existing accounts carefully.

- You must contact EACH credit reporting agency to place the freeze. If you have trouble placing the freeze online, try placing it by phone.
- Remember, if you place the freeze you will need to temporarily or permanently lift it before applying for a good or service that requires a credit check. To lift the freeze, you will need the PIN each credit reporting agency gave you when it was placed. You may also need to lift the freeze if your employer checks your credit report for background purposes.
- The freeze lasts until you lift it and is FREE.

Call all three to place the Freeze.

Call one to place the Fraud Alert.

Equifax: 800-685-1111
TransUnion: 800-680-7289
Experian: 888-397-3742

Check your credit reports. Request yours at www.annualcreditreport.com or by calling 877-322-8228. Go over the reports carefully, marking any information that doesn't belong to you. Dispute incorrect information with the credit reporting agencies.

Place a fraud alert. When you have a fraud alert on your report, a business must verify your identity before it issues credit or services in your name; this makes it harder for a thief to open new accounts in your name. It also allows you to request another free credit report from each credit reporting agency.

Online account safety. Update your online account information often, using strong passwords. Don't share your passwords or use the same ones for all your accounts. Consider using multi-factor authentication, if it's offered. It adds an extra step (like a text message code or finger print) to your login process, making it more secure.

THINKING OUTSIDE THE BOX

Consider these other tools for protecting your accounts. Many banks offer account alerts that can be fitted to your needs. Get a text if your balance falls below a certain number. Get an email or phone call if a charge greater than $50, etc. hits your account. These alerts can make watching existing accounts less of a hassle.

Report charges you didn't make right away. If you wait too long, your bank could make you pay for the charges.

WATCH OUT FOR SCAMS

Don't give your personal information to someone you don't know. Be wary of calls, emails, texts and pop-ups you did not solicit. Scammers can use information taken from a breach to make their request seem legit. When in doubt, cut-off contact and call SCDCA's Identity Theft Unit.