The
South Carolina Department of Consumer Affairs

Presents

IDENTITY THEFT HOW TO AVOID IT AND WHAT TO DO IF IT HAPPENS TO YOU

What is Identity Theft?

Identity theft is the unlawful use of your personal information.

Identity thieves impersonate you and use your information to get credit or money, and for other criminal purposes.

ID Theft Facts

The FTC Estimates That Losses To Business Total $50 Billion Annually.

In The Last Five Years, 27 Million Americans Have Had Their Identity Stolen.

How does it happen?

Thieves get information in a variety of ways:

- From you – when they ask!
- Lost or stolen wallets or receipts
- Preapproved offers
- Dishonest bank,car dealer or credit company employees
- Bogus bank/IRS forms returned to them by unsuspecting consumers
- Discarded or duplicate checks
- Registration information
- Over the Internet

How Do ID Thieves Use the Information?

They call your credit card issuer and, pretending to be you, ask to change the mailing address on your credit card account.

They open a new credit card account, using your name, date of birth and SSN.

They open a bank account in your name and write bad checks on that account.

And They Aren't Done Yet…

They establish phone or wireless service in your name.

They counterfeit checks or debit cards, and drain your bank account.

They buy cars by taking out auto loans in your name.

They give your name to the police during an arrest. If they're released from police custody, but don't show up for their court date, an arrest warrant is issued in your name.

SO WHAT ARE YOU TO DO????

Minimize your risk

Shred unnecessary documents and old receipts, files, and records.

Check your credit report at least once a year.

Don’t give your information to unfamiliar people or businesses.

Ask people why they need the information? What will they do with it? How will they protect it? With whom will they share it?

Protect Your Mail and Trash

Guard your mail and trash from theft. Deposit outgoing mail in post office collection boxes or at your local post office, rather than in an unsecured mailbox. Promptly remove mail from your mailbox.

Stop an identity thief who may pick through your trash or recycling bins to get your personal information: tear or shred information.

And A Few More Tips...

Pay attention to your billing cycles. Follow up with creditors if your bills don't arrive on time.

Be wary of promotional scams. Identity thieves may use phony offers to get you to give them your personal information.

Opt Out When Possible

More organizations are offering people choices about how their personal information is used including an opt-out choice that limits the information shared with others or used for promotional purposes.

Pre-screened Credit Offers

If you receive pre-screened credit card offers in the mail (based on your credit data), tear them up after you decide you don't want to accept the offer.

To opt out of receiving pre-screened credit card offers, call: 1-888-5-OPTOUT (1-888-567- 8688).

In addition, you can notify the three major credit bureaus that you do not want personal information about you shared for promotional purposes.

Telemarketing

The federal government has created the National Do Not Call Registry — the free, easy way to reduce the telemarketing calls you get at home. To register visit www.donotcall.gov, or call 1-888-382-1222 from the phone you want to register.

Mail

The Direct Marketing Association's (DMA) Mail Preference Service lets you "opt- out" of receiving direct mail marketing from many national companies for five years.

E-Mail

The DMA also has an EMail Preference Service to help you reduce unsolicited commercial emails. To “opt-out” of receiving unsolicited commercial email, use DMA’s online form at www.dmaconsumers.org/offemaillist.html

Social Security Numbers

Your employer and financial institution need your SSN for wage and tax reporting purposes. Other businesses may ask you for your SSN to do a credit check. **You don't have to give a business your SSN just because they ask for it.** ASK QUESTIONS!!

A business may not provide the service or benefit you're seeking if you don't provide your SSN. Remember — THE DECISION IS YOURS.

Offline banking: how to keep your money $afe

- Read statements and receipts carefully, then shred what you don’t need.
- Shield your transactions at the ATM.
- Don’t use any suspicious keypads or card swipers.
- Shred old and unused checks.
- If you do find a fraudulent transaction, report it to your bank immediately.

Computer Safety

Do not download files sent to you by strangers or click on hyperlinks from people you don't know.

Use a firewall program to stop uninvited guests from accessing your computer.

Use a secure browser — software that encrypts or scrambles information you send over the Internet. When submitting information, look for the "lock" icon on the browser's status bar to be sure your information is secure during transmission.

ID Theft "Insurance"

- Several companies offer ID theft insurance or protection
- Consumer should be very wary of these contracts
- Consumer should read the policy or contract carefully to determine what is (and is not) covered

What to do if your identity is stolen

If you suspect that your personal information has been misappropriated to commit fraud or theft, take action immediately.

There are four basic actions you need to take appropriate in almost every case.

First Step if your identity is stolen: credit reporting agencies

- Call the toll-free fraud number of any one of the three major credit bureaus to place a fraud alert on your credit report.
- As soon as the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified to place fraud alerts on your credit report, and all three reports will be sent to you free of charge.

Second Step if your identity is stolen: close accounts

- Close any accounts that have been tampered with or opened fraudulently.
- If you're closing existing accounts and opening new ones, use new Personal Identification Numbers (PINs) and passwords.
- If there are fraudulent charges or debits, ask the company for the form to file to dispute the transactions.

Second Step if your identity is stolen, Part 2

- If your checks have been stolen or misused, close the account and ask your bank to notify the appropriate check verification service. You must make the bank aware of the forgery.

- You also should contact the major check verification companies. Ask that retailers who use their databases not accept your checks on the stolen or forged account.

Third Step if your identity is stolen: report to police

- **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.

Fourth Step if your identity is stolen: Federal Trade Commission

- **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 enters the information you provide into a secure database.

For more information on Identity Theft, contact:

The South Carolina Department of Consumer Affairs

1.800.922.1594

www.scconsumer.gov

Federal Trade Commission

www.ftc.gov