ID Theft and Fraud Victim Resource Booklet

SOLID

TAKES RISK DOWN

A PEG OR TWO

SunTrust

Live Solid. Bank Solid.

Contents

Are You Safe from Identity Theft?

Visit us online at suntrust.com

Identity theft is a very real crime, with very real victims, and sometimes life-altering consequences. In a criminal's mind, the person who is diligent about maintaining their credit and making financially responsible decisions is a perfect target.

No matter how conscientious you are about protecting your personal information no one is completely safe from identity theft. Skilled thieves, like pickpockets, burglars and computer hackers, have many ways to obtain your important data to use for their own benefit.

In this guide SunTrust has compiled useful information to help prevent identity theft as well as provide information to those whose identities or personal financial information have already been compromised.
To learn more, the following Web sites are good resources to obtain additional information about identity theft:

Federal Trade Commission — www.consumer.gov/idtheft

Identity Theft Resource Center — www.idtheftcenter.org

Privacy Rights Clearinghouse — www.privacyrights.org

Social Security Online — www.ssa.gov/pubs/idtheft.htm

Fraud Assessment

Do you regularly check each item on your monthly credit/debit card statement?

You should always check your statement, to ensure every transaction is correct. If you notice any irregularities, immediately bring them to the attention of the issuer of the bank card by telephone and in writing.

Is your Social Security number and/or driver's license number listed on your personal checks?

Never list this information on your checks. If your checks get into the wrong hands, criminals can easily steal your identity.

Do you run a regular credit check on yourself?

Running a credit history check on a routine basis can help detect and prevent identity theft before it gets out of control.

Do you go to Web sites by clicking on links within an Email from someone you don't know?

Unless you certain of the Email's source, either call the company on the telephone, or go to the Web site directly by typing the Web address in your browser.

Do you shred unwanted documents containing your personal information before throwing them away?

You should always shred documents containing personal information; otherwise, it could prove useful if it reaches the wrong hands.

Do you check a Web site for the security lock before making purchases?

The ability to recognize a secure Web connection is extremely important; there are two general indications of a secure Web page:

1. Check the Web page URL (Web page address) — normally the URL begins with the letters "http." However, over a secure connection the address displayed should begin with "https" — note the "s" at the end. This lets you know that before you enter sensitive information (username, password, card information, etc.); it will be encrypted before it is sent to the site's server.
2. Check for the "Lock" icon — most Web browsers adhere to a standard where a "lock" icon is displayed somewhere in the window of the browser. Most sites display the lock icon in the lower-right of the browser window; however, the location will vary by Web browser. One more important note — the lock icon is not just a picture; if you click the icon, it should take you to the site's security details.

Is Your Wallet Hurting You?

Having your wallet or purse stolen from you can turn into a real hassle. Should one of these items be stolen, you'll have to cancel your credit cards, notify your bank to order a new check card and checks and you'll also have to get a new driver's license. You may also have to get a new cell phone and change the locks on your house. Here are some items that you should think twice about keeping in your wallet or purse:

Social Security Card

This is the last piece of information you want thieves to have access to. It is best to keep your card stored in a locked box in a safe location.

Business Cards

A business card not only gives away your work information, it can also give thieves an idea of how much your salary may be and whether that address on your driver's license might make a good target for a home burglary.

Large Amounts of Cash

Since you can pay for virtually any item with a debit or credit card, there really is no need to carry around more than $50 for everyday expenses. Remember, once cash is stolen, there is a very slim chance that you will get it back.

More than Two Credit Cards

By limiting the number of cards you carry, you minimize the damage that thieves can do to you.

Checks

Checks contain your name, address, checking account number, routing number, and bank name — all of which can help thieves set up online transfers of money out of your account and into theirs.

Common Fraud Schemes

There are are no new scams — just new victims. It seems that each day con artists add new spins to age-old scams and go in search of victims. Yesterday's snake-oil salesmen are the equivalent of today's phish Emails advertising weight-loss supplements.

So what's the difference? Today's shysters don't go from town to town to entice consumers with loud, rapid-fire, slick pitches. Instead, they invade your home through wireless and cable connections. They wait patiently in your Email inbox, on Web sites, behind nameless, faceless modern technologies.

How do you stop them? By learning the three basic scam types detailed below, you will be able to spot any scam — no matter what new spin it's given by clever con artists.

Remember, fraudsters are clever people whose main goal is to make you part with your hard-earned money. They will use many variations of the scams listed below to do so. By taking the time to educate yourself about these common types of scams, and by sharing this information with others, you can make a valuable contribution to the war against fraud.

PHISHING

A phishing scam attempts to trick would-be victims into providing personal information (account numbers, passwords) to what they believe to be a legitimate company.

However, the Web site address given in the Email link is a “spoof" of the company's official Web site and is unauthorized. Fraudsters then use your personal and account information to commit fraudulent transactions.

Remember, most legitimate companies would not request your sensitive information via Email. It is best to contact a company to verify an Email before you give up your information.

VISHING

Recently, fraudsters have stepped up their efforts to trick people into providing their personal or financial information via the telephone. Fraudsters usually use two common tricks. They either send you an Email that appears to be from your bank requesting you contact them to resolve a situation with your account. Another way is for them to contact you directly.

It is crucial that you never provide this sort of information via phone unless you have initiated the call. If you receive this type of call or Email, call the business using a phone number you know is legitimate.

ADVANCE FEE

You may receive an Email, letter, or fax that asks for your help in order to access a large sum of money located in a foreign bank account. The message says you will get a percentage of the funds in exchange for your help.

This message is an example of the type of scam known as a Nigerian or “419” scam. The “large sum of money” does not exist. Those who respond to the scam messages will eventually be asked for advance fees supposedly required to allow the deal to proceed.

If you receive one of these scam Emails, do not respond to it; it is best to delete the Email.

GENERAL SCAM INDICATORS

The general rule of thumb is this: if something sounds too good to be true, it probably is.

Be wary of unsolicited Emails that:

- Promise you money, jobs or prizes for very little on your part
- Ask for donations
- Propose lucrative business deals
- Ask you to provide sensitive personal information
- Ask you to follow a link to a Web site and log on to an account

How Do They Use My Information?

Once someone has your personal information, there are many ways they can use it without your knowledge:

- Imposters can call your card issuer pretending to be you and ask to change the mailing address on your account. They'll then run up charges on your account. Because your statements are being sent to the new address, it may take some time before you realize there is a problem.
- Thieves can open a new credit card account using your name, date of birth and Social Security number. When they use the credit card and don't pay the bills, the delinquent account is reported on your credit report.
- Establish utility services, phone/wireless services in your name.
- Opening bank account(s) in your name and writing fraudulent checks to drain your bank account.

Secure Your Personal Information

At SunTrust, we are committed to working with you to protect your personal information. Here are some easy things you can do to prevent someone from stealing your important information.

Carry Only What You Need in Your Wallet

The less personal information you have on you, the better.

Don't Put Outgoing Mail in an Unsecured Mailbox

Thieves will often drive around looking for unsecured mailboxes to steal mail. It is best to drop your mail into a secure, official Postal Service collection box.

Report Lost or Stolen Credit Cards Immediately

Call each credit card issuer and ask to have the account closed and open a new account. Remember to update any automatic payment accounts with your new account numbers.

Don't Preprint Personal Information on Checks

Your checks should not have your driver's license, telephone or Social Security numbers pre-printed on them.

Report Lost or Stolen Checks Immediately

SunTrust will block payments on the check numbers involved. Also, review new checks to make sure none have been stolen in transit. Review your account for counterfeit checks and to ensure the checks that clear the bank were written by you.

Be Careful with Your ATM and Credit Card Receipts

Thieves can use them to access your accounts. Never throw away receipts in a public trash can.

Guard Your Personal Identification Numbers (PINs) and Passwords

Don’t write your PIN on your ATM or credit cards and don’t keep your PINs with your cards. We strongly recommend that you don’t create PINs or passwords using information that can be guessed easily (i.e., birthdays, addresses or pets’ names). Don’t share PINs or passwords with friends or family. It is best to change passwords frequently.

How to Handle Identity Theft

You can recover from identity theft. In fact, if you suspect that you may be a victim, you've already taken an important first step by contacting a SunTrust Fraud Specialist.

We will give you and your fraud case the personalized attention it deserves and work with you every step of the way. We'll also assist you as you work with credit bureaus and other key agencies.

In the event you are a victim of fraud, identity theft or burglary, there are a number of steps you can take to help ensure your personal and financial interests are protected:

- Immediately contact your bank and credit card issuer to verify that access to your accounts are limited to you and authorized users.
- Place stop payments on missing checks.
- Change PIN and online banking passwords.
- Open new account(s) as appropriate.
- Request that a fraud alert be placed in your credit bureau file.
- Inform the credit bureaus to include a statement on your credit report asking that creditors call you before opening any new accounts or changing your existing accounts.

You can attach up to 2 contact phone numbers, and you can remove an alert at any time. Initial Alerts remain on file for 90 days (Opt-out remains on file for 90 days).

An Extended Alert requires a law enforcement report and remains on file for 7 years (Opt-out remains on file for 5 years). Active-Duty Alerts remain on file for active duty military consumers for 1 year (Opt-out remains on file for 2 years).

Ask for copies of your credit reports and review them carefully. If you are a victim of identity theft, credit bureaus are obligated to give you a free copy of your report to check for inaccuracies. Make sure that no additional fraudulent accounts have been opened or unauthorized changes made. Check the inquiry section of the report. When inquiries appear from companies that opened fraudulent accounts, request that the inquiries be removed from your report. Then follow up with the credit bureaus and any associated financial institutions to ensure the information they contain is up-to-date.

Placing a fraud alert on your credit report indicates you are (or may be) the victim of identity theft. This fraud alert signals to lenders and creditors to exercise extra precaution before granting credit using your name and credentials.

Agencies to Contact

Credit Reporting Agencies

EQUIFAX
P.O. Box 74021
Atlanta, GA 30374
Order Report: 800.685.1111
Report Fraud: 800.525.6285
www.equifax.com

EXPERIAN
P.O. Box 2002
Allen, TX 75013
Order Report: 888.397.3742
Report Fraud: 888.397.3742
www.experian.com

TRANSUNION
P.O. Box 2000
Chester, PA 19022
Order Report: 800.888.4213
Report Fraud: 800.680.7289
www.transunion.com

Merchant Check Guarantee Firms

These agencies will place information in their systems about checks that are reported as lost/stolen or opened fraudulently. Merchants who accept checks as a form of payment often subscribe to this type of service in order to validate the information on the check.

Certegy Check Services:	800.770.3792
Telecheck Services, Inc.:	800.366.2425
International Check Services:	800.526.5380
SCAN:	800.262.7771

Social Security Services

The Social Security Administration has established a hotline for victims of identity theft to report misuse of a Social Security number. You may also visit your local Social Security office for further information.

SSA Hotline: 800.269.0271

Local SSA Office Information: ____

____

Department of Motor Vehicles (DMV)

If your driver's license has been stolen, it is important to report the theft immediately to your DMV. Reporting the theft in a timely manner will help ensure that a duplicate license is not issued to an imposter.

Web Site: www.dmv.org

Local DMV Information: ____

____

Other Support Agencies for Fraud Victims

U.S. Postal Inspection	www.usps.com/postalinspectors
Federal Trade Commission	www.ftc.gov or www.consumer.gov/idtheft
Department of the Treasury	www.identitytheft.gov

Identity Theft Prevention Checklist

□ **Edit Your Wallet**	Think about what you really need on a daily basis such as your driver's license, one credit and/or debit card, cash, checkbook. It is vitally important to protect your Social Security number; never carry your Social Security card in your wallet or put your number on your checks. When your Social Security Number is requested, ask why it's needed. Double-check your current driver's license and your health insurance policy card. If your Social Security number is included, ask to be given another number.
□ **Invest In a Shredder**	It is amazing the lengths to which some identity thieves will resort to in order to retrieve your personal information, including digging through your trash. Before disposing of receipts, old credit card statements, or other personal documents — take a few seconds to run them through a shredder. If you don't have a shredder, it is best to tear them into the tiniest pieces possible. This will discourage thieves from taping them back together.
□ **Secure Your Personal Information**	You wouldn't leave a stack of cash laying around, so why leave sensitive materials around the house? To secure personal information, consider investing in a fire-proof safe or a file cabinet which can be locked. Don't relax your guard at work either: be sure to stow your purse or wallet in a desk drawer or a cabinet which can be locked.
□ **Monitor Your Accounts**	Be proactive by monitoring your financial accounts on a regular basis. Most financial institutions offer online banking so you can see pending and posted transactions as they are made. Also, ask if your credit/debit card company offers fraud alerts; most offer it for free while others may require a slight fee. These programs are very helpful since they alert you when there are any abnormal purchases or activity on your account.
□ **Credit Freeze**	This option prevents credit card companies and other third parties from viewing your credit report. Keep in mind that while this gives you a little more protection than a fraud alert, you'll need to lift the freeze if you want to apply for a loan or a credit card.
□ **Passwords**	Use a mix of letters, numbers, and special characters to create a foolproof password, and alter it for every online account you have. One way to outwit fraudsters is to create a complicated password. Think of a catchy phrase that is special to you and use only the first letter of each word, incorporating a special character and number at the end. For example: "I graduated from Central High School number 1." Password: "igfchs#1." And for each Web site, change the number or a character, or add letters corresponding to the particular Web site. So when you visit, say, a retail Web site, your password would be "taigfchs#1."

How to Report Fraud

If you suspect suspicious or fraudulent activity regarding any of your SunTrust accounts, please report the suspicious or fraudulent activity by doing the following:

If You Suspect the Following:	Then:
• Lost or Stolen Checks • Unauthorized Check/Paper Draft Activity • Lost or Stolen Check Card or ATM Card • Unauthorized ACH Withdrawal • Unauthorized Debit Card Transaction • Unauthorized Wire Transfer	Call the Fraud Assistance Center at 1.800.447.8994. To expedite your call, please be sure you have the following information available: • Account Number and/or Check Card Number • Date and Amount of Fraudulent Transaction • Pen/Paper to Record Your Case Number
Fraud involving your: • Equity Line • Consumer Loan • Small Business Loan	Call the Consumer Lending Operations Fraud Department at 1.877.239.3149.
Lost or Stolen Personal SunTrust Credit Card	Call Card Services Customer Service at 1.800.477.9702.
Lost or Stolen Commercial Card	Call 1.800.836.8562.
Suspicious SunTrust Emails (Phishing) or Scams	Forward information about the Email, pop up Web page and/or scam to emailabuse@suntrust.com. You will receive an automated response to let you know we received your Email. If you believe that you have provided personal or account information in response to a fraudulent Email or site, please contact a SunTrust representative immediately at 1 800 SUNTRUST? (1.800.786.8787).

Social Networking Safety Tips

Social networking sites have become the newest meeting spaces for online users. From Facebook to MySpace to Twitter, these sites enable people to connect with their friends, family, coworkers and many others in order to share information such as photos, videos, and personal messages. While it is very easy to make new friends through these sites, there are some precautions you should take to protect yourself from hackers, identity thieves and the like.

Guard Your Info

This may seem like common sense but sometimes users of social networking sites get lulled into a false sense of security and familiarity because they are communicating with people they trust. However, it is always best to never provide or post your Social Security number, address, phone number, bank account or credit card numbers, or other personal information that could be used by criminals. Also, be careful to not post details such as when you're on vacation — thieves may use that information to burglarize your home. One way to prevent strangers from seeing your information is by setting your profile to private or adjusting the privacy settings on the networking site.

Think Twice before Clicking on Links or Downloading Attachments in Emails

The reality is, you can't always know if an Email is from a trusted source because hackers can break into accounts and use them to send messages. An example of this would be a friend urgently needing money or sending you a link to a video that requires you to download a player in order to view it. These types of messages often contain viruses or spyware that could not only damage your PC but are designed to steal your personal information.

If you receive a questionable message from a friend, it's best to use an alternative method to contact them to find out if they really sent the message. If you get a message from a stranger, it is best not to click on any links or attachments that may be embedded in the Email.

Third Party Applications

Many social networking sites allow you to download third party applications that let you personalize your page. Before you download any files or applications, ensure your PC is protected. Make sure your security software and operating system software is updated. Before downloading any attachment or software, take a moment to ask yourself if you really know and trust the sender.

Meeting New Friends

Sometimes people you are interacting with online may not be who they say they are. Fraudsters are increasingly turning to social networking sites to look for potential victims. If someone you just met online wants to meet you in person, be cautious and do your research. It's a good idea to see what background you can dig up through online search engines. Also, be selective about who you choose to befriend on social networking sites.

For more information, visit: http://www.ftc.gov/bcp/edu/pubs/consumer/tech/.tec14.shtm.

Before signing up with a social networking site or even if you've already signed up with one, take the time to read their privacy policies so you are aware of how your information is being stored and shared.

Also, be aware of who has access to your profile. While most social networking sites come with default privacy settings, it is always best to view your settings and customize it so that you control the way your information can be accessed and shared with others. Another rule of thumb is to act as if anything you post online can be read by anyone who visits that Web site. When you consider that this information can be seen by others such as law enforcement and current or prospective employers, you may think twice about what you post.

Online Security

Protect Your PC

In 2008, more than $264 million was lost due to internet fraud! These figures represent a 33% increase in complaints and a $25 million increase in losses over 2007. Email and Web pages were the two primary mechanisms scammers used to commit their crimes. The Federal Bureau of Investigations (FBI) recommends several steps to protect your computer and yourself from being a victim:

Keep Your Firewall Turned On

A firewall helps protect your computer from hackers who might try to gain access to crash it, delete information, or even steal passwords or other sensitive information. Software firewalls are widely recommended for single computers. The software is prepackaged on some operating systems or can be purchased for individual computers. For multiple networked computers, hardware routers typically provide firewall protection.

Install or Update Your Antivirus Software

Antivirus software is designed to prevent malicious software programs from embedding on your computer. If it detects malicious code, like a virus or a worm, it works to disarm or remove it. Viruses can infect computers without users' knowledge. Most types of antivirus software can be set up to update automatically.

Install or Update Your Anti-spyware Technology

Spyware is just what it sounds like — software that is surreptitiously installed on your computer to let others peer into your online activities. Some spyware collects information about you without your consent or produces unwanted pop-up ads on your desktop. Some operating systems offer free spyware protection, and inexpensive software is readily available for download on the Internet or at your local computer store. Be wary of ads on the Internet offering downloadable anti-spyware — in some cases these products may be fake and may actually contain spyware or other malicious code. It's like buying groceries — shop where you trust.

Update Your Operating System

Computer operating systems are periodically updated to stay in tune with technology requirements and to fix security holes. Be sure to install the updates to ensure your computer has the latest protection.

Be Careful What You Download

Carelessly downloading Email attachments can circumvent even the most vigilant anti-virus software. Never open an Email attachment from someone you don't know, and be wary of forwarded attachments from people you do know. They may have unwittingly forwarded malicious code.

Turn Off Your Computer

With the growth of high-speed Internet connections, many opt to leave their computers on and ready for action. The downside is that being "always on" renders computers more susceptible. Beyond firewall protection — which is designed to fend off unwanted attacks — turning the computer off effectively severs an attacker's connection, be it spyware or a botnet that employs your computer's resources to reach out to other unwitting users.

For more information, visit: www.fbi.gov/cyberinvest/protect_online.htm

Learn the Terms

Adware

A type of software that often comes with free downloads. Some adware displays ads on your computer, while some monitors your computer use (including Web sites visited) and displays targeted ads based on your use.

Browser Hijacker

A common spyware program that changes your Web browser's home page without the user's knowledge, even if you change it back.

Cookies

A small text file that a Web site can place on your computer's hard drive to collect information about your activities on the site or to allow the site to remember information about you and your activities.

Drive-by Download

Software that installs on your computer without your knowledge when you visit certain Web sites. To avoid drive-by downloads, make sure to update your operating system and Web browser regularly.

Hacker

Someone who uses computers and the Internet to access other people's computers without permission.

Keystroke Logger

A device or program that records each keystroke typed on a particular computer.

Malware

A combination of the terms "malicious" and "software," used to describe any software designed to cause damage to a single computer, server, or computer network. Criminals sometimes use malware — programs like viruses and spyware — to get into your computer, and once there, they can steal information, send spam, and commit fraud. Learn to spot the signs of malware and what you can do to reclaim your computer and your electronic information.

Online Profiling

A scam that involves Internet fraudsters who send spam or pop-up messages to lure personal information (credit card numbers, bank account information, Social Security number, passwords, or other sensitive information) from unsuspecting victims.

Peer-to-Peer (P2P)

A method of sharing files, usually music, games, or software, with other users through a sharing program that allows uploading and downloading files from other users online. Caution should be used as P2P sharing can lead to downloading dangerous files as they are often misrepresented and can contain offensive material, malware, viruses, or other unintended items; trusted scanning software should always be used.

Phishing

A scam that involves Internet fraudsters who send spam or pop-up messages to lure personal information (credit card numbers, bank account information, Social Security numbers, passwords, or other sensitive information) from unsuspecting victims.

Spam Zombies

Home computers that have been taken over by spammers without the consent or knowledge of the computer owner. The computers are then used to send spam in a way that hides the true origin.

Social Networking Sites

Websites that allow users to build online profiles and share information, including personal information, photographs, blog entries, and music clips, and connect with other users, whether to find friends or land a job.

Spyware

A software program that may be installed on your computer without your consent to monitor your use, send pop-up ads, redirect your computer to certain Web sites, or record keystrokes, which could lead to identity theft.

Trojans

Programs that, when installed on your computer, enable unauthorized people to access it and sometimes to send spam from it.

TRUSTe

An online seal program. Websites displaying the seal have agreed to abide with certain principles regarding user privacy. You can access the site's privacy policy by clicking on the seal.

suntrust.com
800.227.3782

SunTrust

Live Solid. Bank Solid.

SunTrust Client Commitment: SunTrust will never send unsolicited Emails asking clients to provide, update, or verify personal or account information, such as passwords, Social Security numbers, PINs, credit or Check Card numbers, or other confidential information.