Online Fraud & Identity Theft Guide

A Guide to Protecting Your Identity and Accounts

SunTrust

At SunTrust, we're committed to protecting your accounts and identity. That's why we've created this Identity Theft Guide. This guide provides information about online fraud and identity theft, as well as an action plan of what to do if your identity has been stolen.

Although it's not possible to completely prevent identity theft or online fraud, you can help protect your personal information and accounts by using caution when providing confidential information and following the tips included in this guide.

What's Inside…

What Is Identity Theft?

Identity theft is a serious crime that occurs when someone illegally obtains and uses pieces of your personal information for their own gain. Information like your name, address, date of birth, Social Security Number, Internet Banking passwords and PINs, and credit and Check Card numbers can be keys to your financial information. When scammers obtain your confidential information, they can charge expenses to your accounts, create new accounts in your name or use your personal information for other illegal purposes.

How Your Identity Can be Stolen

Identity thieves look for the same thing - pieces of your personal information. Here are just a few examples of how they might obtain your identity:

- **Searching your trash.** This is called “Dumpster Diving” - a term to describe people who rummage through your trash to find unshredded information like credit card offers, old bills and bank statements.

- **Intercepting your mail.** They can complete “change of address” forms and receive mail that’s intended for you.

- **Stealing your wallet or purse.** Your wallet or purse can contain a wealth of information about you, including your account numbers, Social Security Number, address and date of birth.

- **Copying your account numbers during purchases.** Your credit and debit card account numbers can be stolen when your card is swiped for purchases. Scammers use special hand-held devices to record your account information.

- **Accessing your employer’s files.** Your place of work stores a lot of your personal and business information. This can be a target for identity thieves.

- **Getting information directly from you.** Sometimes, thieves pose as telemarketers, or someone who might have a legitimate reason to ask for your personal information (like your bank, employer or landlord.) They even use fake emails and Web sites to try and obtain information from you.

Signs of Identity Theft

Identity theft is dangerous because it can remain hidden for a relatively long time before it's identified. Here are some signs to help you identify if you've been a target of identity theft:

- **Missing mail**. A telling sign of identity theft is if you are missing mail or see a significant drop in amount of mail you receive.
- **Suspicious transactions.** Monitor your accounts, statements and credit reports and look for unusual transactions.
- **Unexpected declines.** Be alert to any unexpected declines for a loan or mortgage despite your good credit.
- **Strange calls.** Calls from a collection agency or business about merchandise or services you don't recognize are another sign that someone has stolen your identity.
- **New credit cards**. A credit card in the mail that you didn't apply for could be a sign that someone has attempted to steal your identity.

Help Protect Yourself from Identity Theft

It's important to remember to use caution when disclosing personal and financial information. There are a number of ways you can help protect yourself from identity theft:

- ✓ **Sign the back of your credit and debit cards.** This minimizes the possibility of someone else using your card.
- ✓ **Keep your credit card receipts**. Don't throw your receipts away. They can help you double check your bank and card statements and identify any suspicious activity.
- ✓ **Report lost or stolen credit or ATM cards immediately.** If you lose your credit or ATM cards or if they are stolen, it's important that you contact your bank immediately.
- ✓ **Cancel and destroy all unused cards and checks.** Discard credit cards and checks you don't use. Call the banks to cancel the cards and destroy the cards before throwing them out. When you destroy the cards and checks, make sure the numbers are no longer recognizable.
- ✓ **Leave out personal information on your checks.** You don't need to include your driver's license, telephone or Social Security Number on your checks. By omitting this information, you keep confidential information away from prying eyes.
- ✓ **Don't leave your mail laying around**. Your incoming mail has clues to your personal information. Make sure you collect it promptly.
- ✓ **Shred your junk mail.** Make sure you shred all your junk mail before you throw it away – especially credit card offers which could contain confidential information.
- ✓ **Don't drop your outgoing mail in your mailbox.** It's safer to drop your outgoing mail in official Postal Service collection boxes – especially if your mailbox is not locked.
- ✓ **Review your credit reports.** Make sure they're error-free. There are three credit-reporting agencies whose reports can show different information. It's best that you review them at least once a year for any suspicious activity.

  - o Equifax 1-800-525-6285 or http://www.equifax.com
  - o Experian 1-888-397-3742 or http://www.experian.com
  - o TransUnion 1-800-680-7289 or www.transunion.com

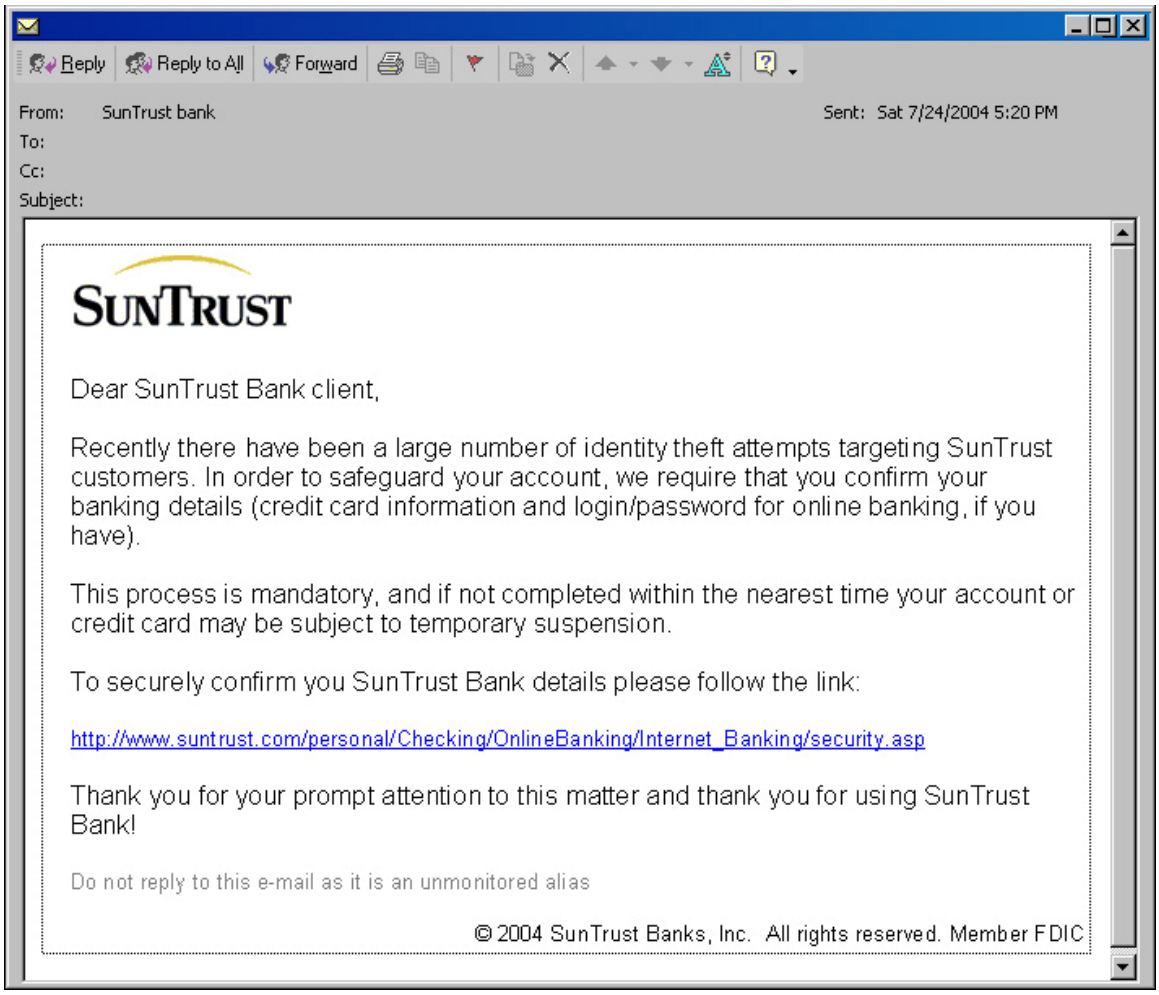
- ✓ **Don't respond to unsolicited requests for personal or account information.** Unsolicited email and pop-up Web page requests for personal information can be dangerous. If a request seems suspicious, call the company to check it out.

- ✓ **Keep your personal information in a safe place.** Don’t store a list of credit card numbers, PIN numbers or passwords in your wallet or on your computer. Memorize this information.

Be on the Lookout for Online Fraud

A popular form of online fraud is “phishing” (sounds like “fishing”). Scammers use fraudulent emails or pop-up Web pages that often look like they are from legitimate businesses to deceive you into sharing personal or account information. When you respond to these online scams, you jeopardize the security of your accounts and your identity can be stolen. You should never provide your personal or account information in response to unsolicited emails or pop-up Web pages.

Here is an example of a fraudulent email:



Reply | Reply to All | Forward

From: SunTrust bank
Sent: Sat 7/24/2004 5:20 PM
To:
Cc:
Subject:

SUNTRUST

Dear SunTrust Bank client,

Recently there have been a large number of identity theft attempts targeting SunTrust customers. In order to safeguard your account, we require that you confirm your banking details (credit card information and login/password for online banking, if you have).

This process is mandatory, and if not completed within the nearest time your account or credit card may be subject to temporary suspension.

To securely confirm you SunTrust Bank details please follow the link:

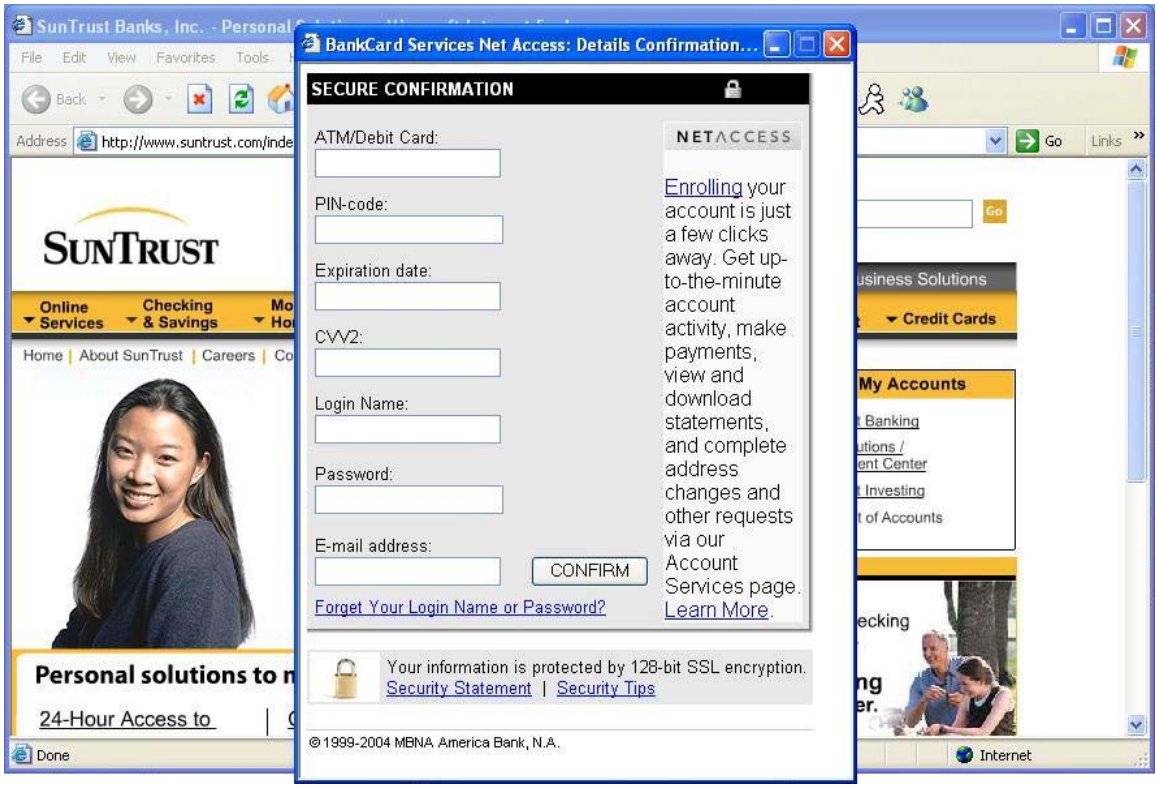
http://www.suntrust.com/personal/Checking/OnlineBanking/Internet_Banking/security.asp

Thank you for your prompt attention to this matter and thank you for using SunTrust Bank!

Do not reply to this e-mail as it is an unmonitored alias

© 2004 SunTrust Banks, Inc. All rights reserved. Member FDIC

Here is an example of a fraudulent Web page:



How Do Scammers Obtain Your Email Address?

Many scammers randomly generate email addresses – that's why you may have received fraudulent emails that appear to be from banks you do not have accounts with. Scammers also collect personal and account information through viruses embedded in emails. In addition, they also purchase mailing lists through legitimate means and collect emails from the Internet through Web pages, chat rooms, online auctions and directories. *SunTrust does not trade, rent or sell our clients' personal information – including email addresses – to anyone*.

Help Protect Yourself from Online Fraud

There are many things you can do to help secure your identity and your accounts. Here are some tips:

- ✓ **Look beyond the logo.** To make fraudulent emails or Web sites appear real, scammers often include actual logos and images of legitimate companies. They also convey a sense of urgency, stating that if you fail to provide, update or verify your personal or account information, access to your accounts will be suspended. It's important that you look beyond the logo and not give out your information.

- ✓ **Use your spam filter.** Many email services now have spam filters that minimize the amount of unsolicited and unwanted emails you receive. The filters can help you minimize the number of fraudulent emails in your inbox.

- ✓ **Type, don't click.** Even if you open a suspicious email, don't click on any links. By clicking on the links you could inadvertently download a virus or spyware to your computer. Even if you think the email is legitimate, type Web addresses into your browser instead of clicking on links. If the email is from an institution you do business with, use a bookmark that you've already created to visit that company's Web site.

- ✓ **Change your online passwords often.** The rule of thumb is to change your password every 30 to 60 days. Try and be creative with your passwords – stay away from obvious passwords like your zip code, year of birth or sensitive information such as your mother's maiden name or your Social Security Number.

- ✓ **Update your anti-virus and anti-spam software.** By keeping anti-virus and anti-spam software up to date on your computers, you make it more difficult for scammers to access your personal and account information. Most anti-virus and anti-spam providers offer subscription services to ensure that you receive the latest software updates. If you're not sure if your software is up to date, contact your anti-virus or anti-spam provider.

How SunTrust Helps Safeguard Clients' Information

We're committed to keeping our clients' accounts safe from unauthorized access and their identities confidential. We use industry-standard technologies on our Web site, such as encryption, firewalls, and pass codes to protect our clients' personal and account information.

At SunTrust, we have strict privacy policies in place. SunTrust does not trade, rent or sell our clients' personal information – including email addresses – to anyone. We do not provide account or personal information to non-SunTrust companies for the purpose of independent telemarketing or direct mail marketing for non-financial products or services. For more information on our privacy policy, visit https://www2.suntrust.com/privacy.html.

SunTrust Client Commitment

SunTrust will **never** send 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.

How to Report Online Fraud

- ✓ To report a suspicious email or Web page, forward information to reportfraud@suntrust.com.
- ✓ If you believe you have provided personal or account information in response to a fraudulent email or Web site, immediately contact a SunTrust representative at **1-800-227-3782** or visit www.suntrust.com/alert and complete the "Online Fraud Form."

You are the best protection against identity theft and online fraud. By staying informed and using caution when you disclose confidential information, you can help protect your identity and accounts. For more information about online fraud, visit www.suntrust.com/alert.

If You're a Victim of Identity Theft

If you think you're a victim of identity theft, take these steps immediately:

- **Notify one of the three major credit bureaus and place a fraud alert on your credit report.** Call the toll-free fraud number of any of the three major credit bureaus to place a fraud alert on your credit report. This can help prevent an identity thief from opening additional accounts in your name. Once the credit bureau confirms your fraud alert, the other two credit bureaus will automatically be notified.

- **Contact your financial institutions and credit card companies**. Close the affected accounts with unauthorized withdrawals or charges and open new ones with new personal identification numbers and passwords.

- **Contact the local police department and ask to file a miscellaneous incident report**. Even if the police do not catch the criminal, having a police report can help you clear up your credit records. Ask for the case number and a copy of the report.

- **Contact all the businesses that have opened accounts in your name without your permission.** Close the accounts and let the businesses know that the accounts were opened fraudulently. Make sure you communicate with the businesses in writing.

- **Notify the Federal Trade Commission.** Call 1-877-ID-THEFT (438-4338) or visit www.consumer.gov/idtheft. By sharing your identity theft complaint with the FTC, you will provide important information that can help law enforcement officials track down identity thieves.

- **Report stolen mail.** File a report with the Postal Service. Call your local Postal Inspector or visit www.usps.com.

- **Report a stolen SSN.** Call the Social Security Fraud Hotline at 1-800-269-0271.

- **Report stolen checks.** If your checks have been stolen or misused, close all affected accounts and contact these check verification companies:

TeleCheck	1-800-710-9898
Certegy	1-800-437-5120

- **Alert the Securities and Exchange Commission (SEC) at 1-800-732-0330.** If you identify suspicious activity in your investment accounts, contact the SEC immediately.

At the end of this guide is a worksheet to help you document your notifications to credit bureaus, law enforcement officials, businesses and financial institutions that your identity has been stolen.

SUNTRUST

Sample Dispute Letters

If you become a victim of identity theft, you can use the following sample letters to dispute charges made to your accounts. All of your communications should be written and you should make copies of all of your correspondence for your files.

Sample Dispute Letter for Credit Bureaus*

Date

Your Name
Your Address
Your City, State, Zip Code

Complaint Department
Name of Credit Bureau
Address
City, State, Zip Code

Dear Sir or Madam:

I am writing to dispute the following information in my file. The items I dispute are also circled on the attached copy of the report I received. (Identify item(s) disputed by name of source, such as creditors or tax court, and identify type of item, such as credit account, judgment, etc.)

I am a victim of identity theft, and did not make the charge(s). I am requesting that the item be blocked to correct my credit report.

Enclosed are copies of (use this sentence if applicable and describe any enclosed documentation) supporting my position. Please investigate this (these) matter(s) and block the disputed item(s) as soon as possible.

Sincerely,

Your name

Enclosures: (List what you are enclosing.)

*Source: Federal Trade Commission at *http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm*

Sample Dispute Letter for Existing Credit Accounts*

Date

Your Name
Your Address
Your City, State, Zip Code
Your Account Number

Name of Creditor
Billing Inquiries
Address
City, State, Zip Code

Dear Sir or Madam:

I am writing to dispute a fraudulent (charge or debit) attributed to my account in the amount of $_____. I am a victim of identity theft, and I did not make this (charge or debit). I am requesting that the (charge be removed or the debit reinstated), that any finance and other charges related to the fraudulent amount be credited as well, and that I receive an accurate statement.

Enclosed are copies of (use this sentence to describe any enclosed information, such as police report) supporting my position. Please investigate this matter and correct the fraudulent (charge or debit) as soon as possible.

Sincerely,

Your name

Enclosures: (List what you are enclosing.)

*Source: Federal Trade Commission at http://www.ftc.gov/bcp/conline/pubs/credit/idtheft.htm

Learn More About Online Fraud and Identity Theft

The best way to protect yourself against identity theft and online fraud is to use caution when providing personal and account information and to stay informed about scams. Following are a few useful links for additional information:

- ✓ SunTrust: www.suntrust.com/alert
- ✓ FTC Consumer: www.consumer.gov/idtheft
- ✓ U.S. Department of Justice: www.usdoj.gov/criminal/fraud/idtheft
- ✓ USPS Postal Inspectors: www.usps.gov/postalinspectors
- ✓ FTC Spam: www.ftc.gov/spam

Credit Bureaus - Report fraud to at least one of the credit bureaus and order a copy of your credit report

Bureau	Phone Number	Date Contacted	Person Contacted	Comments
Equifax	1-800-525-6285			
TransUnion	1-800-680-7289			
Experian	1-800-397-3742			

Law Enforcement Authorities - Report Identity Theft

Agency	Phone Number	Date Contacted	Person Contacted	Comments
Local Police Department				
Federal Trade Commission	1-877-IDTheft or www.ftc.gov			
Social Security Administration	1-800-269-0271			
U.S. Postal Service	Local Post Office			

Banks, Credit Card Issuers and Other Creditors

Creditor	Address and Phone Number	Date Contacted	Contact Person	Comments
SunTrust Identity Theft Services Group	1-866-493-3446 Option 2			

SUNTRUST