SunTrust
Seeing beyond money

Online Fraud and Identity Theft Guide

A Guide to Protecting Your Identity and Accounts

As part of SunTrust's commitment to protecting your accounts and identity, we've created the Online Fraud & Identity Theft Guide, which provides information about preventing online fraud and identity theft, as well as steps to take if your identity has been stolen.

Although it may not be possible to completely prevent identity theft or online fraud, you can help protect your personal information and accounts by 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 personal information for their own gain. Your name, address, date of birth, Social Security number, Online Banking passwords and personal identification numbers (PINs), and credit and check card numbers are keys to your financial information. When scammers obtain this 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

Here are a few examples of how scammers might obtain your identity:

- **Searching your trash** to find unshredded information such as credit card offers, old bills, or bank statements.
- **Intercepting your mail** by completing change-of-address forms and receiving mail that's intended for you.
- **Stealing your wallet or purse** which can contain a wealth of information about you, including your account numbers, Social Security number, address, and date of birth.
- **Copying your account numbers** after your card is swiped for purchases using special hand-held devices.
- **Accessing your employer's files** which contain a lot of your personal and business information.
- **Getting information directly from you** by posing as telemarketers, or someone who might have a legitimate reason to ask for your personal information (such as your bank, employer, or landlord). They also use fake email and Web sites to try to obtain information from you.

Signs of Identity Theft

Identity theft is dangerous because it can occur without your knowledge. Here are some ways to help you identify whether you've been a target of identity theft:

- **Missing mail** – If you believe you are missing mail or see a significant drop in the amount of mail you receive, you may be a victim.
- **Suspicious transactions** – Monitor your accounts, statements, and credit reports and look for unusual transactions.
- **Unexpected declines** – Look for any unexpected declines in 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 Prevent Identity Theft

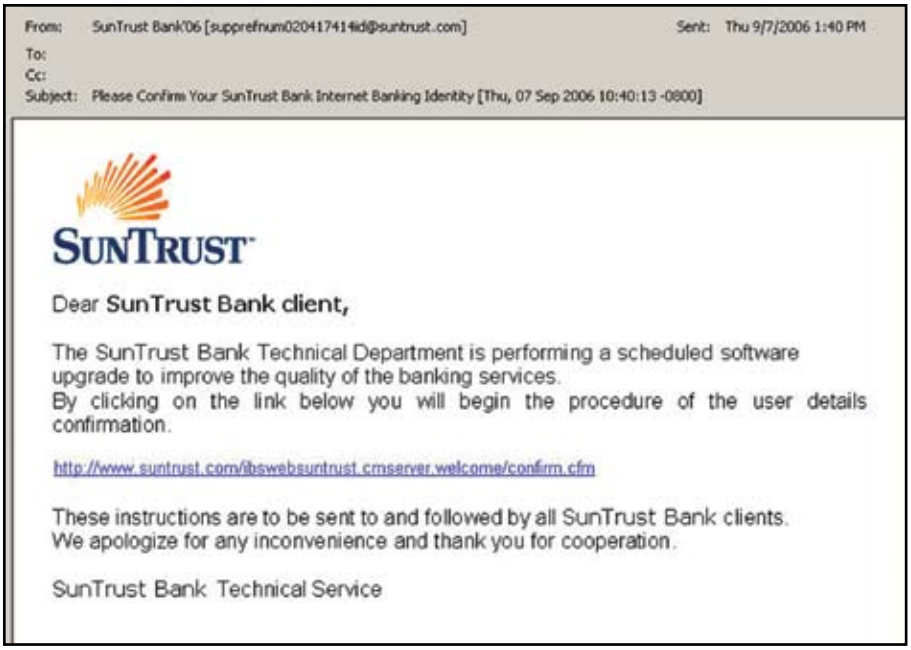
It's important to use caution when disclosing personal and financial information. There are a number of ways you can help protect yourself from identity theft:

- **Sign the back of your credit and debit cards.** This minimizes the possibility of someone else using your card.
- **Keep your credit and debit card receipts.** Use them to double-check your statements and identify any suspicious activity.
- **Report lost or stolen credit or debit cards immediately.** If your credit or debit cards are lost or stolen, it's important to contact your bank immediately.
- **Cancel and destroy all unused cards and checks.** Discard credit cards and checks you don't use. Call your bank to cancel the cards and destroy them before discarding. When you destroy the cards and checks, make sure the numbers are not recognizable.
- **Do not print 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 lying around.** Your incoming mail includes personal information; make sure you collect it promptly.
- **Shred your junk mail.** Be sure to shred all junk mail before throwing 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 to review them at least once a year for any suspicious activity.
  - Equifax 800.525.6285 or equifax.com
  - Experian 888.397.3742 or experian.com
  - TransUnion 800.680.7289 or 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, PINs, or passwords in your wallet or on your computer. Commit this information to memory.

Be on the Lookout for Online Fraud

A popular form of online fraud called phishing (pronounced "fishing") is the use of fraudulent emails or pop-up Web pages to entice you to share 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 personal or account information in response to unsolicited emails or pop-up Web pages.

Here are examples of fraudulent emails:



From: SunTrust Bank'06 [supprefnum020417414id@suntrust.com] Sent: Thu 9/7/2006 1:40 PM
To:
Cc:
Subject: Please Confirm Your SunTrust Bank Internet Banking Identity [Thu, 07 Sep 2006 10:40:13 -0800]

SUNTRUST

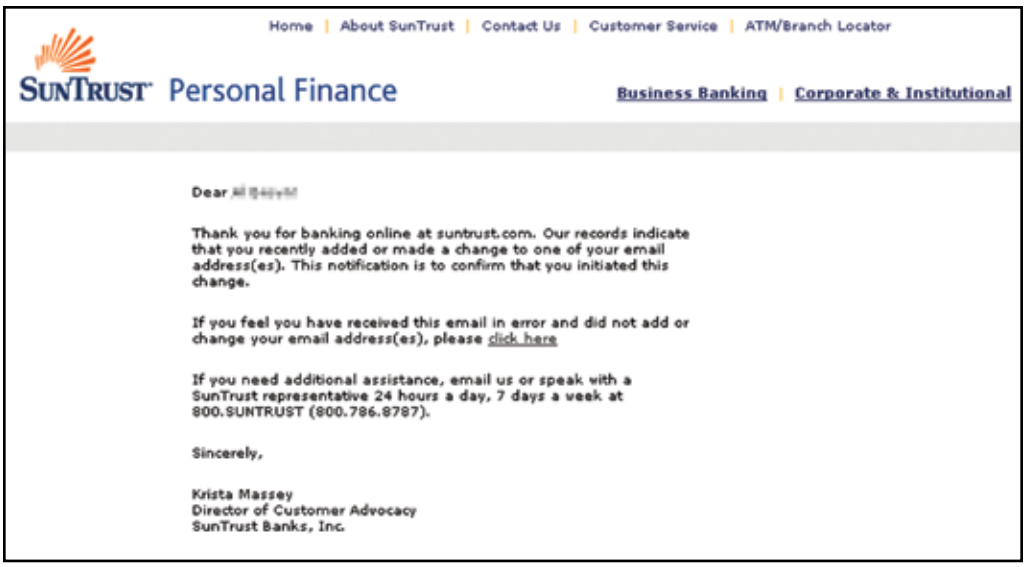
Dear **SunTrust Bank client,**

The SunTrust Bank Technical Department is performing a scheduled software upgrade to improve the quality of the banking services.
By clicking on the link below you will begin the procedure of the user details confirmation.

http://www.suntrust.com/ibswebsuntrust.cmserver.welcome/confirm.cfm

These instructions are to be sent to and followed by all SunTrust Bank clients.
We apologize for any inconvenience and thank you for cooperation.

SunTrust Bank Technical Service



Home | About SunTrust | Contact Us | Customer Service | ATM/Branch Locator

SUNTRUST Personal Finance

Business Banking | Corporate & Institutional

Dear [redacted]

Thank you for banking online at suntrust.com. Our records indicate that you recently added or made a change to one of your email address(es). This notification is to confirm that you initiated this change.

If you feel you have received this email in error and did not add or change your email address(es), please click here

If you need additional assistance, email us or speak with a SunTrust representative 24 hours a day, 7 days a week at 800.SUNTRUST (800.786.8787).

Sincerely,

Krista Massey
Director of Customer Advocacy
SunTrust Banks, Inc.

Here is an example of a fraudulent Web page:

This fraudulent Web site looks exactly like the SunTrust homepage, but the first characters of the URL are not https://www.suntrust.com.

How Do Identity Thieves Obtain Your Email Address?

Identity thieves send fraudulent emails at random that appear to be from a bank with which you may or may not have an account. They also collect personal and account information through viruses embedded in emails, or they may legitimately purchase mailing lists and collect emails from the Internet through Web sites, chat rooms, online auctions, or directories.

Our privacy policy states that SunTrust does not trade, rent, or sell our clients' personal information – including email addresses – to anyone.

Help Prevent Online Fraud

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

- **Look beyond the logo.** To make fraudulent emails or Web sites appear real, identity thieves 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. Ignore the legitimate appearance of these Web sites and resist giving out your information.
- **Use your spam filter.** Many email services now have spam filters that minimize the amount of unsolicited emails you receive. These filters can help you minimize fraudulent emails in your inbox.
- **Type, don't click.** If you do open a suspicious email, don't click on any links – you could inadvertently download a virus or spyware to your computer. Even if you think the email is legitimate, type the Web address into your browser instead of clicking on the link. If the email is from an institution you do business with, use a bookmark you've already created to visit that company's Web site.
- **Change your online passwords every 30 to 60 days.** Get creative with your passwords – stay away from the obvious such as 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 computer, 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 Safeguards Clients' Information

We're committed to keeping our clients' accounts safe from unauthorized access and their identities confidential. We use industry-standard Web technology, such as encryption, firewalls, and pass codes.

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 suntrust.com/privacy.

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.

How to Report Online Fraud Regarding Your SunTrust Account

- To report a suspicious email or Web page, forward it to reportfraud@suntrust.com.
- If you have provided personal or account information in response to what you believe to be a fraudulent email or Web site, contact a SunTrust representative immediately by calling 800.227.3782 or visit suntrust.com/alert and complete the Online Fraud Form.

You are your own 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 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 accounts with unauthorized withdrawals or charges and open new ones with new PINs and passwords.
- **File a miscellaneous incident report with the local police department.** Even if the police do not catch the criminal, having a police report can help you clear up your credit report. Ask for the case number and a copy of the report.
- **Contact all 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 (FTC).** Call 877.ID.THEFT (438.4338) or visit 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 usps.com.
- **Report a stolen Social Security number.** Call the Social Security Fraud Hotline at 800.269.0271.
- **Report stolen checks.** If your checks have been stolen or misused, close all affected accounts and contact the following check verification companies:

  TeleCheck 800.710.9898
  Certegy 800.437.5120

- **Alert the Securities and Exchange Commission (SEC) at 800.732.0330.** If you identify suspicious activity in your investment accounts, contact the SEC immediately.

This guide includes a worksheet to help you document notifications of identity theft to credit bureaus, law enforcement officials, businesses, and financial institutions.

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 communications should be in writing 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: FTC at 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, 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: FTC at 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. Please visit these links for additional information:

- SunTrust: suntrust.com/alert
- FTC (consumer): consumer.gov/idtheft
- USPS inspectors: usps.gov/postalinspectors
- FTC (spam): 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	800.525.6285			
TransUnion	800.680.7289			
Experian	800.397.3742			

Law Enforcement Authorities – Report Identity Theft

Agency	Phone Number	Date Contacted	Person Contacted	Comments
Local Police Department				
Federal Trade Commission	877.IDTheft or ftc.gov			
Social Security Administration	800.269.0271			
U.S. Postal Service	Local Post Office			

Banks, Credit Card Issuers, and Other Creditors

Creditor	Address and Phone Number	Date Contacted	Person Contacted	Comments
SunTrust Identity Theft Services Group	866.493.3446, option 2			