


suntrust.com
800.SUNTRUST



 SunTrust Bank is an Equal Housing Lender. Member FDIC.
©2010 SunTrust Banks, Inc., SunTrust, Live Solid. Bank Solid.,
SunTrust Rewards, and Signature Advantage Checking, are federally
registered service marks of SunTrust Banks, Inc. DGD111029-10
316435 03/10

PERSONAL

Tips for Safe Banking

SOLID

IS WHERE

SAFE MEETS SOUND



SUNTRUST

Live Solid. Bank Solid.

At SunTrust, we believe protecting your accounts and identity is a partnership. That's why we've put together these tips to help you learn more about identity theft and fraud.

Why It's Important to Protect Your Personal Information

It's important to always use caution when providing anyone with your personal or account information. Personal information such as your Social Security number, account numbers, passwords, or PINs are keys to your finances. If criminals obtain your personal or account information, it's possible they can withdraw funds from your bank account, create new accounts in your name, apply for loans or credit cards, or even assume your identity.

Safeguard Your Personal and Account Information

It's important to keep the following information safe and secure:

- Social Security number
- Driver's license
- Military ID
- Account numbers
- Credit card numbers
- Date of birth
- Passport
- Online security questions and answers
- PINs
- Check Card numbers
- Address
- Birth certificate
- Green card
- Passwords
- Student ID
- Mother's maiden name

At SunTrust, the protection of your assets - including your identity - is our top priority. That's why we're the first major financial institution to offer Equifax Credit Watch™ Silver identity theft protection free when you open a select personal checking account.* Discounts on Equifax Credit Watch products are available for all personal checking accounts. Visit suntrust.com/creditwatch to sign up for an Equifax Credit Watch product.

How Criminals Obtain Your Personal and Account Information

Criminals often try to take advantage of trusting people in a number of ways, including:

- **On the phone.** Criminals may state they are calling on behalf of your financial institution with concerns about your account. They may claim they need your information in order to protect your account, or that you've won a cash prize and your account number is needed so they can deposit the money.
- **By fax.** Criminals may send a fax inviting you to take advantage of a special offer, such as a low interest rate on a home loan. The fax may instruct you to contact a bank representative immediately, and ask you to provide your personal and account information. To look official, the fraudulent faxes may include the logo of a legitimate company.
- **By mail.** Not only can criminals steal mail out of an unsecured mailbox, they can complete change-of-address forms, allowing them to receive mail intended for you. Some criminals search your trash to find unshredded information like credit card offers, old bills, and bank statements.
- **In person.** Criminals can access your information by stealing your wallet or purse or by copying your credit card numbers during in-store and restaurant purchases.

* One Equifax Credit Watch Silver subscription for one person per account for Solid Choice Checking or Signature Advantage Checking accounts. Discounts on Equifax Credit Watch products available for all other personal checking accounts.

- **In newspapers.** Fraudulent advertisements may offer great deals on home loans. The fake ads often include logos of legitimate companies and provide a phone number for readers to call to apply for the loan. When readers call, criminals collect personal and account information, and may request “advance payments.”
- **Online.** Some criminals use the Internet to obtain confidential information. A popular form of online fraud is called phishing (pronounced “fishing”). Criminals use fraudulent emails or pop-up Web pages designed to entice you to share personal or account information.

How online fraud works:

Criminals often send fake emails that look like they’re from legitimate companies. These emails or pop-up Web pages may ask you to provide, update, or verify your personal or account information, telling you that if you do not update your information, access to your accounts will be restricted. If you respond to these online scams, you jeopardize the security of your accounts.

How criminals obtain your email address:

Many criminals randomly generate email addresses using software. Some collect personal and account information through viruses embedded in emails. Others purchase mailing lists or 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.

Tips for Safe Banking

Following are some tips on how to help protect your accounts and identity:

Mail

- Don't leave your outgoing mail in an unsecured mailbox. Drop your outgoing mail in a post office mailbox or take it to a post office.
- Keep track of your mail. If a statement, check, or bill is missing, contact the company that sends you the mail immediately. Check to see if your address has been changed without your authorization.
- Tear up or shred credit card offers that you receive in the mail, as well as expired cards. Before throwing them away, make sure the account numbers are no longer readable.
- Review your bank and credit card statements carefully. Report any discrepancies or missing statements to your financial institution immediately.
- Sign up to receive Paperless Online Statements and eBills – electronic versions of your bills – through Online Banking with Bill Pay.

Direct Deposit eliminates the risk of lost, stolen, or delayed checks in the mail, helps protect people from identity theft, and is reliable in times of disaster. And it is the fastest way to receive regular payments directly into your checking account, including Social Security checks, pension payments, and payroll checks. Ask your banker for a Direct Deposit form to provide to your employer. If you receive Social Security or other government payments, visit godirect.org to sign up online or call **800.333.1795**.



Credit and Check Cards

- Sign the back of your credit and check cards as soon as you receive them.
- Immediately report lost or stolen cards to your credit card issuer.
- Order your credit report from at least one of the three credit bureaus once a year to check for fraudulent activity or other discrepancies. If you see unauthorized transactions, contact at least one of the credit bureaus immediately:

1. **Equifax:** 800.525.6285 or equifax.com
2. **Experian:** 888.397.3742 or experian.com
3. **TransUnion:** 800.680.7289 or transunion.com

- Don't create passwords or PINs that can be easily guessed, such as your ZIP code, date of birth, or pet's name. Also, avoid using sensitive information such as your mother's maiden name or your Social Security number. Use a combination of letters and numbers, and change your passwords and PINs every 30 to 60 days. Immediately change your passwords and PINs if you suspect your accounts have been compromised.
- Never share your password and PINs with anyone, even SunTrust employees. Never write your passwords or PINs anywhere, especially on your card. Safeguard your credit card account numbers and do not keep a list of account numbers in your purse or wallet.

ATMs and Night Depositories

- Avoid going to the ATM alone at night. If you do need to access your accounts after dark, make sure the ATM and parking lot are well-lit.
- If you make regular deposits at the ATM, keep a supply of deposit envelopes on hand so you can have them filled out before you reach the ATM.
- Have your ATM or check card out and ready to use before you reach the ATM.
- Don't use an ATM if you notice any suspicious activity. If you do notice something suspicious, find another ATM or come back at a later time. Immediately report any suspicious activity to the police or the branch manager.
- Don't count your money at the ATM. Wait until you are safely in your car.
- When using a drive-up ATM, keep your doors locked, passenger windows rolled up, and the car running.
- Don't open locked ATM entrances or doorways for others. Authorized clients should have their own access card.
- Make sure you have your card, receipt, and cash before you leave the ATM.
- Keep your ATM receipts and record the transactions in your checkbook.
- If you use the night depository, have your night deposit bag and commercial key ready when you approach the depository. Once you've placed the bag in the depository, open it again to make sure your bag went down the chute.

On the Internet

- Never provide personal or account information in response to unsolicited emails or pop-up Web pages.
- Many fraudulent, unsolicited emails and pop-up Web pages appear real because they use logos of legitimate companies. It's important to look beyond the logo and resist giving out sensitive information.
- Type Web addresses into your browser window instead of clicking on links in emails. If you click on links in emails, you could be taken to fraudulent sites that look authentic or you could unknowingly download a virus or spyware to your computer.
- Select online security questions and answers that are relevant to you and easy to remember but difficult for others, including your family to guess.
- Change your passwords and PINs every 30 to 60 days. If you suspect your accounts have been compromised, change your passwords and PINs immediately.
- Install and keep the latest security software up-to-date on your computer. This software also makes access to your personal and account information more difficult. In addition, consider using a personal firewall. It can help prevent attacks against your computer.
- Use online banking to monitor your accounts. SunTrust's Online Banking with Bill Pay provides you access to your accounts 24/7, so you can quickly identify any suspicious activities and notify the bank. SunTrust Online Banking with Bill Pay is free – and is a completely guaranteed way to pay your bills safely and securely. SunTrust guarantees that your payments will arrive on time – on the dates you tell us – as long as you schedule the payment properly,** or SunTrust will pay your late fees.

** In accordance with the Bill Payment Scheduling guidelines described in the Online Banking/PC Banking terms and conditions.

To sign up for Online Banking with Bill Pay:

- Visit suntrust.com/signup, call **800.382.3232**, or visit your local SunTrust branch to sign up for Online Banking.
- Once you have signed on to Online Banking, simply access the “Pay Bills” tab to begin using SunTrust Online Bill Pay.
- Receive your statements online. SunTrust offers Paperless Online Statements through Online Banking. Paperless Online Statements provide safe, secure access to your detailed transaction and balance information. Paperless Online Statements provide:
 - Email notification when statements are ready to view.
 - The ability to view, print, and save statements as soon as they are ready.
 - Access up to 18 months of deposit account statements online.

To turn off your paper statements, visit suntrust.com and enter your “User ID” and “Password” in the Online Banking box located in the top left corner of the Personal Finance homepage.

- Select “Turn on/off paperless statements” under “I want to...” in the upper right-hand corner.
- Select the “No” under “Receive Paper Statements.”
- Select “Update Statement Delivery Preferences.”

Learn More About Safe Banking

The best way to help protect your identity and accounts is to always use caution when disclosing personal and account information, and to stay up-to-date about the latest fraud and identity theft scams. To learn more, visit suntrust.com, which offers additional tips, updates, and valuable information about how to help protect your identity and accounts.

SunTrust at Your Service

At SunTrust, we take fraud and identity theft as seriously as you do. We have dedicated resources in place to assist you. Following is a quick list of contacts in case you need help:

If you suspect the following...

- Lost or Stolen Checks
- Unauthorized Check/Paper Draft Activity
- Lost or Stolen Check Card or ATM Card
- Unauthorized ACH Withdrawal
- Unauthorized Wire Transfer

Fraud involving your:

- Equity Line
- Consumer Loan
- Small Business Loan

Lost or Stolen Personal SunTrust Credit Card

Lost or Stolen Commercial Credit Card

Suspicious SunTrust emails (phishing) or scams

Potentially fraudulent phone call

I need to order a credit report

SunTrust recommends:

Call our fraud specialty group STOLI **800.447.8994**. You can also contact SunTrust at **800.SUNTRUST (800.786.8787)**.

Call the Retail Lending Fraud Department at **877.239.3149**.

Call Card Services Customer Service at **800.477.9702**.

Call **800.836.8562**.

Forward information about the email, pop up web page or scam to **emailabuse@suntrust.com**.

If you believe you have provided personal or account information in response to a fraudulent email or site, please contact a SunTrust representative at **800.SUNTRUST (800.786.8787)**.

If you believe you have provided personal or account information in response to a fraudulent phone call, immediately call **800.SUNTRUST (800.786.8787)**.

SunTrust provides Equifax Credit Watch Silver for free with one of the following accounts:

Solid Choice Checking
Signature Advantage

This service can help you monitor your credit information and detect any unauthorized access. It's offered at a discounted price with other personal checking account types. To subscribe, please visit **suntrust.com/creditwatch** or contact Equifax at **866.798.1148, Option 1**.

For other helpful information, go to **suntrust.com** and select "Help Protect Your Accounts and Privacy" on the right-hand side of the Personal Finance page.