

SCAMS 101: How to Protect Yourself From Scams



At SunTrust, we're committed to protecting your identity from theft and fraud. We know you work hard for your money and want to help ensure you don't become a victim of a scam that could result in financial loss. This introductory guide provides vital information on what a scam is, how to avoid common types of scams, and how you can help protect yourself from becoming a victim of a scam in the future.

What's Inside

- **How to Protect Yourself From Scams**

- An Introduction
- Lottery Scams
- Inheritance Scams
- Work-From-Home Opportunities
- Overpayment for Goods or Services
- High-Profit, No-Risk Offers
- Relationship Scams

- **How SunTrust Protects You**

- **How to Help Protect Yourself**

- **Learn More About Scams**

- **Contact Us**

What is a scam?

A scam is a type of fraudulent activity based on the deceit of someone who intentionally misleads another person or people, usually with the goal of financial gain. A typical scam occurs when individuals are tricked into thinking there's an opportunity to earn or receive extra money quickly and easily.

Different types of popular scams include:

- Lotteries – especially from foreign countries
- Inheritances
- Work-from-home opportunities
- Overpayment on sold items
- High-profit, no-risk offers
- Relationship scams

If it sounds too good to be true, it probably is.

Have you been scammed?

You may have been scammed if you answer “yes” to any of the following questions.

Lotteries

- Have you been informed that you are the winner of a lottery – even one that you did not play?
- Have you received a lottery check in the mail?
- Have you been instructed to wire, send, or ship money as soon as possible to a large U.S. city or another country such as Canada, England, or Nigeria?

Inheritances

- Have you received a letter notifying you that you will receive an inheritance?
- Have you been asked to deposit part of your inheritance and then send back a portion of the money to cover fees or in order to receive the rest of your inheritance?

Work-From-Home Opportunities

- Have you been offered employment to work from home and make a large salary or commission?
- Have you been asked to hold or transfer money for a profit or commission?

Overpayment for Sold Items

- Have you received a check for an item that you sold on the Internet that was more than the selling price of the item?
- Is the check you received for the item associated with an email communication from someone you didn't know before the transaction?

High-Profit, No-Risk Offers

- Have you received an unsolicited phone call, email, or letter from someone you don't know?
- Have you responded to radio or television infomercials to earn money quickly?

Relationship Scams

- Has someone you met online asked you for money in order to remedy a traumatic situation?
- Has someone you met online asked you to negotiate a check, travelers check, or money order on their behalf at your bank?

General Tips to Avoid Being Scammed

Remember, if an offer appears too good to be true, it probably is. Here are some general tips to help protect you:

Avoid disclosing personal or financial information. Don't share personal or account information such as account numbers, check card numbers, Social Security numbers, or any other sensitive information with strangers.

Look out for suspicious Web sites. Watch out for copycat sites that may try to look like financial institutions or other trusted companies that you do business with. To make sure you're visiting a legitimate site, type the business' address directly into your browser, or use a bookmark that you previously created.

Be wary of low- or no-risk offers. Some advertisements offer something for free or low-cost. These "free" offers could commit you to further financial obligations.

Know who you are doing business with. It's a good idea to research the companies that solicit your business. The Better Business Bureau has information on more than 2.5 million organizations available online. If you can't find any company information during your research, consider this a red flag and avoid doing business with them.

Avoid high pressure situations or deadlines. If someone urges you to act quickly or advises you not to tell anyone else, you should be cautious about a relationship with them. You have the right to take time to decide whether you'd like to participate in any kind of transaction or business venture.

Don't wire money. If a potential employer, unconfirmed business solicitor, or potential buyer asks you to wire them money – don't do it! It's a scam.

Guaranteed quick profits are rare. Be suspicious of anyone who claims they can generate guaranteed profits quickly. They hope you will jump at the chance to participate in their scheme.

Be leery of lottery and inheritance notifications. More likely than not, it is a scam.

Lottery Scams

One of the most popular and fastest growing forms of fraud is the lottery scam. In this type of fraud, the scammer wants you to believe that you have won a substantial amount of money in a lottery – even one in which you did not participate. Advances in technology have enabled con artists to create documents that look authentic, including official-looking checks and award letters.

Lottery scams are generally delivered via U.S. mail, although there are variations that are received over the Internet or phone.

Example Letter/Check from a Lottery Scam:



Types of Lottery Scams

A lottery scam may fall into one of the following categories:

Foreign Lottery

Some lottery scams originate from other countries, such as Canada or the Netherlands.

It Looks Official, But It's Not

Many lottery schemes appear to be from reputable companies or financial institutions. Letters can include phone numbers and request that you immediately contact an organization to confirm your winnings. The documentation you receive may also contain a check that looks authentic.

Pay to Participate

Scammers may ask you to deposit their check and then return a portion of the money to cover fees or taxes associated with your winnings. Usually, the sum requested for payment is relatively small compared to the full amount you've supposedly won. Legitimate lotteries do not ask you to pay fees to secure your prize. If you cash the check, you could be responsible for any bank fees.



Here are a few tips to help you avoid lottery scams:

- If you didn't play a lottery, you didn't win.
- If it's a foreign lottery, ignore the communication.
- Lotteries don't require winners to pay fees to collect their winnings.
- Never give out personal or financial information to anyone who tells you you've won a lottery over the Internet or phone.
- Be skeptical of unsolicited calls, emails, or letters informing you that you've won.

Inheritance Scams

Inheritance scams try to deceive you into believing that a long-lost relative has passed away and left you a large sum of money. You may receive an email from a “research specialist” or a notice informing you of your good fortune. These notifications often ask you to send a check to help cover expenses associated with your inheritance. However, if you send a check, you’re not only out of the money you send, but also an inheritance that never existed.

Although there is no one single inheritance scam method, the intent and general premise is the same: an unclaimed inheritance has been located and you’re an heir to the money. Scammers will go so far as to look up your family tree information online to find a recognizable name from your family’s past.

The individual or organization who notifies you of your inheritance states they will send you details about how to claim your inheritance – for a fee. Most of these scams are delivered via mail, and increasingly by email. A smaller number of them are circulated by newspaper advertisements, which usually claim to try to “find the rightful heirs” of huge estates.

You can help protect yourself from inheritance scams by:

- Carefully reviewing all unsolicited regular mail and email
- Checking with relatives about recent deaths in your family
- Limiting giving out personal information on the Internet

Example Letter from an Inheritance Scam:

Dear Sir,

I am C.D. Mann, a designated legal representative of a group of business partners who would like to approach you regarding a recent discovery about your family. It has been determined that one deceased ~~Mr. K. Bridges~~, who died recently of natural causes, has only you and your family as living relatives. Due to your distinct relationship to him, it is apparent from our research that you are eligible to receive uncollected monies now currently being held in several bank accounts. The amount of each account is substantial – and will need your attention immediately in order to prevent upcoming holding penalties.

For a small portion of the money due you, our team will release all information to you regarding each account, and work with you to secure all of your funds. I will need to know your intentions regarding this matter. Please call my assistant, Mr. Todd at the following number so that we can resolve the matter. He can also answer any question you may have regarding your inheritance.

Kurt Todd, Esq. 1-888-222-3333

We are glad to partner with you to resolve this and get your family funds to you.

Best Regards,

Work-From-Home Opportunities

Being your own boss while working from home is certainly a dream for many, and that's why work-from-home scams are so lucrative.

Scammers offer easy money with the promise of working from home by advertising online, on the side of the road, or in newspapers. These schemes are often advertised as "Be your own boss," "Work from home," or "Make extra money."

Work-from-home scams take many forms and can include "businesses" such as medical billing, envelope stuffing, or working for a vendor. Individuals who sign up to work for these "businesses" run the risk of being paid late, very little, or not at all. Further, con artists can use the information you provide them – such as your name, address, Social Security number, etc. – to commit fraud or identity theft.

Before you provide information about yourself when presented with an employment opportunity:

- Use common sense. If a particular job seems too good to be true, it probably is.
- Most companies don't require you to pay money to work. Don't waste your time or money.
- Ask detailed questions about the type of work you will be doing, how you will be getting paid, when you will be getting paid, etc.



Example Letters/Check from a Work-From-Home Scam:

IMPORTANT: READ CAREFULLY BEFORE PROCEEDING

Please be advised that by accepting this employment offer you are bonded to abide with the following Code of Business Conduct and Ethics.

CODE OF BUSINESS CONDUCT AND ETHICS
Adopted by the Board of Directors, as revised, on March 17, 2005

The Shopping Group is committed to maintaining the highest standards of business conduct and ethics. This Code of Business practices and the principles of expect every employee to read and understand performance of his/her business responsibilities.

Every employee is expected to develop a letter of this Code may be subject to discipline of violation may range from reprimand in appropriate cases civil legal action or

1. HONEST & ETHICAL CONDUCT

It is the policy of the Company to promote all affairs in an honest and ethical manner. **your assignments confidential at all times** targeted business of the evaluation being reputation of the Company depends on job by each person associated with us, to corporate integrity.

2. LEGAL COMPLIANCE

Disobeying the law, both in letter and in success depends upon each employee's with local, national, and international and understand the legal and regulatory requirements of responsibility. Disregard of the law and foreign laws, rules and regulation may result in civil and/ or criminal penalties.

Daid Surveys

1327 Alicanna St., Baltimore, MD 21202 Phone: (410) 366-6661 Fax: (410) 366-6661

October 17, 2006

Ladine A. Ladley

We are a **SECRET CUSTOMER** employment firm that specializes in the assisting of corporations on how to improve customer service to their clientele; we represent 1250 firms with more to come, we utilize a method known as mystery shopping to achieve this goal.

CONGRATULATIONS!!! Due to the information we have ascertained, you have been chosen to represent our company as a secret shopper, in addition you fit the criterion of an individual who is prepared to supplement their income by taking advantage of this opportunity.

The first probational training task is a **PAID** training assignment and is to be completed as directed by any of our assignment co-ordinators, **so please contact us at (410) 366-6661 for detailed instructions.** Your job description would be to pose as a potential customer to the assigned place of business and evaluate the effectiveness, efficiency and customer service of the particular establishment. For the Western Union and Moneygram assignments, you will pose as a potential customer sending a payment to **David Ladley**, a relative of yours in **Baltimore, MD**. In the process of this evaluation, please take note of the quality of service in order to be able to fill out a fair and unbiased opinion on the **Customer Service Evaluation Tool (CSET)** form enclosed with this letter. This form and all receipts must be faxed back to our office upon completion of assignment.

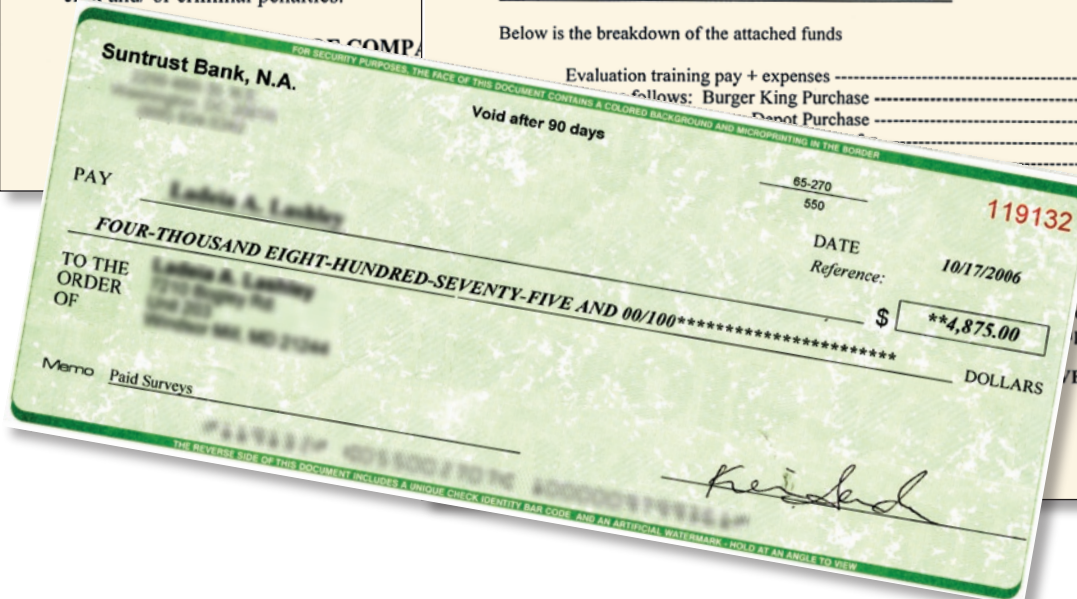
NOTE: ENCLOSED IS A CASHIER'S CHECK FOR \$4,875 TO ASSIST YOU WITH YOUR ASSIGNMENT; IT IS IMPERATIVE THAT UPON RECEIPT OF THIS CHECK THAT YOU CONTACT OUR OFFICE IMMEDIATELY. FAILURE TO COMPLY WILL RESULT IN THE AUTOMATIC STOP PAYMENT ORDER OF CHECK.

Below is the breakdown of the attached funds

Evaluation training pay + expenses	\$881.00
Follows: Burger King Purchase	\$20.00
Follows: Dollar Store Purchase	\$300.00
Follows: Target Purchase	\$2000.00
Follows: Home Depot Purchase	\$99.00
Follows: Wal-Mart Purchase	\$1500.00
Follows: Home Depot Purchase	\$75.00
TOTAL	\$4875.00

ents in addition with you as
 yee Code of Business
 d be performed in a
 ployment opportunity.

BE FUN!! HAVE FUN!!



Overpayment for Goods or Services

Spring cleaning is particularly satisfying when you can turn unwanted items into cash. However, selling these items on an online auction site or in the classifieds could make you the target of an overpayment scam. In these schemes, someone poses as a buyer and replies to your classified advertisement or online auction posting.

The method may differ, but these scams share one characteristic: You have been overpaid for goods provided or services rendered. The scammer offers to purchase the item or service with a check or money order but makes a payment for more than the item's purchase price.

The reasons given could include:

- A mix-up resulted in the wrong amount being sent.
- A portion of the service is no longer required and he or she would like a partial refund.
- The check or money order was originally made out to another business charging a higher rate, but it fell through.

The check you receive is not real, but is usually not detected by bank staff. The scammer asks you to wire back or send a check with the difference after the overpaid amount has been deposited into your account. However, the check or money order will be returned as counterfeit and the "extra" money sent to the "buyer" is lost, along with any already-shipped goods.

Here are some tips to avoid check overpayment scams:

- Never accept a check for more than the purchase price of the product or service.
- If a buyer refuses to send the correct amount, return the check and do not send the merchandise.
- Never agree to wire back funds to a buyer.
- Wait for the buyer's check to clear before sending the items they purchased.



Example Letter from an Overpayment Scam:

Dear Mam,

thanks for the quick response am okay with price, and because am far away from united states so don't worry about the shipment i have shipping agent that carter for my pick up any where in the world. i will instruct my client to send you a cashier's cheque of (5000) so what you have to do immediatley the check gets to you just deduct the funds for the puppies(\$500) and send the excess money (\$4500) to my shipping agent so that they can be able to pick the puppies up from your destination and which will also covers the shipping fees of my other consignments in the state. so if this is okay by you, you can forward your full name, address and cell phone number. expecting your response back.

Sir,

Thanks for your mail, I am really interested in the (plymouth), Fine i will pay \$200 for it, Please i will want to indicate my mode of payment to you since i am not in the United States at the moment and there is a Company in the United States that is indebted to me in the amount of \$3,500. So i will want to really seek your Assistance at this point, That i will want you to forward to me the the following informations below that i will need to forward to the Company indebted to me so that they can make out the payment directly to you and after you have cashed it in your bank, You will have the excess amount on the payment sent to my International Shipping agent via WESTERN UNION MONEY TRANSFER, All charges you are to pay at the western union office when sending the excess amount of \$3,300 should be deducted from my balance. So you don't have to bother yourself about that, The reason for this is that, The Company indebted to me say they cannot make out the payment in two installment except once, And since i am purchasing your (plymouth) from you at this time, I will want to really be sure that my funds will be safe in your hands as i will want to entrust my money unto your care, So inorder for us to complete the purchase of the (plymouth) now, I will want you to get back to me with the following informations inorder for me to forward it to the Company indebted to me inorder for them to make out the payment in your name and send it to you ithout any furtherdelay,

The following informations that i will require from you are as follows,

- 1] YOUR FULL NAME TO BE WRITTEN ON THE CHECK,
- 2] YOUR DIRECT HOUSE ADDRESS WHERE YOU WILL WANT THE PAYMENT TO BE SENT TO,
- 3] YOUR DIRECT CELL PHONE NUMBER THAT YOU CAN BE REACHED AT ANYTIME OF THE DAY SO THAT I CAN GIVE YOU A CALL SO THAT I CAN EXPLAIN TO YOU BETTER,

Upon receipt of this informations i have just requested from you, I will immediately forward it to the Company indebted to me to make out the payment in your name and send it to you immediately, I will be awaiting your response as soon as you get this mail, Do confirm this mail and get back to me as soon as possible.

Thanks

High-Profit, Low-Risk Offers

High-profit, low-risk offers attempt to solicit investments or loans for an emerging business or trading venture. They promise to make you rich with very little risk on your part.

These schemes range from dealing with gemstones, rare coins, and oil and gas leases, to investments in precious metals and art. Scammers are usually seasoned at presenting false claims, and often attempt to build emotional relationships with potential victims, including customers close to retirement who are seeking to secure their financial future.

Common warning signs for this type of scam include:

- Investments that promise quick returns
- Little or no risk associated with the investment
- A limited-time offer – you may miss a “once in a lifetime” opportunity

Separating truth from fiction in these sophisticated schemes is not easy. It helps to do your homework when considering making an investment of any kind.

To help protect yourself from becoming a victim, consider the following tips:

- Be wary of all promises to quickly generate guaranteed high profits.
- Avoid unsolicited promotions, particularly those that don’t provide understandable and detailed explanations of investments.
- Research, research, research. Check with your local Better Business Bureau to make sure there are no negative reports about the solicitor or the investment program. Even if there aren’t any, seek to independently verify the solicitor’s history.



Example Letter from a High-Profit, Low-Risk Scam:

From: chenyuanchimicalcompany chenyuanchimcal@yahoo.comhk

Sent: Tuesday, January 30, 2007 4:44 am

To: xxxxxxxxxxxx

Cc

Bcc

Subject: Update from CHENYUAN CHEMICAL COMPANY LIMITED

Like I told you in my earlier mail, we are major exporters of raw materials from Taiwan. And we are seeking representatives in America, Canada, parts of Europe and Australia that will serve as our Foreign payment receiving officers.

No expertise or financial obligation is required of you in this contract. All we need from you is to submit the following to us;

1. Your complete names,
2. Your complete mailing address(es)
3. Your phone contacts. All of which you have already made available.

The rationale for this is not far-fetched; Most of our overseas customers prefer to pay us in cheques for goods supplied. And here in Taiwan, we have a very slow process in clearing foreign cheques and drafts.

When you are successfully accredited as our foreign payment receiving officer, you shall have the responsibility of clearing all cheques and drafts sent in from America.

You shall get 10% of any payment that is made to us through you. Which you shall deduct immediately after clearance before transferring our balance to our account.

I have forwarded your contact details to the company's account department for accreditation and I shall get back to you in a few hours.

Sincerely,
Shi Lee Hun

YM - ???????????

??

<http://messenger.yahoo.com.uk>

Relationship Scams

The Internet provides the opportunity to establish both business and personal relationships. Scam artists often exploit this opportunity by preying on individuals who frequent Internet chat rooms, online dating services, and social or business networking sites.

A relationship is established with a potential victim, usually by requesting emotional support for a difficult circumstance. By doing this, the scammer slowly cultivates a relationship that they hope will translate into significant goodwill and financial gain.

The relationship may continue for weeks or even months. After a successful online courtship, the scammer will often ask the victim to assist them financially in order to remedy some traumatic situation.

The reasons could include:

- The individual or a family member needs medical attention.
- The individual is a victim of a violent crime and they've been robbed of their belongings.
- The individual would like to visit but needs funding for airline tickets, visas, or customs fees.

Whatever the situation, the scammer asks the victim to send them money, travelers checks, money orders, or some other item to negotiate. They instruct the victim to wire the funds to a third party such as a doctor or hotel manager. It's likely that any proposed transaction will involve counterfeit or altered items.

Here are some tips to avoid relationship scams:

- Be cautious when meeting people on the Internet. Remember, they can pretend to be someone they aren't.
- Do not negotiate items on behalf of someone else.
- Do not send a money transfer to someone you do not know.



Example Internet Conversation from a Relationship Scam:

Andrew8613 – Instant Message

Bethann21: Do you know you are more precious to me then anything in the world?

Bethann21: ?

Andrew8613: I love you too.

Andrew8613: Did you get the package?

Bethann21: Yes, but I thought you said they were money orders but they are travelers checks.

Bethann21: I thought you could cash travelers checks anywhere.

Andrew8613: They couldn't get the cashed here cause they no nothing about it

Andrew8613: That is why I bought them in the first place

Bethann21: Ok

Bethann21: I was not sure

Andrew8613: And they couldn't cash them

Bethann21: I have never used them but I have always heard you could cash them anywhere.

Bethann21: Okay I understand

Bethann21: I just wanted to ask

Andrew8613: Anywhere in canada, mexico, and not African or asian or european countries

Bethann21: Okay baby.

Bethann21: I will go to the bank after I pick the kids up.

Bethann21: I'm kind of smiling right now because this weekend we will be together.

Andrew8613: Ok in a few minutes will you go?

Bethann21: I don't know.

Andrew8613: It is alright take your time my dear ok?

Bethann21: I will need to get some work done here first. I'm sorry

Andrew8613: No apologies. I spoke to the agent and he is waiting.

Andrew8613: Did you fill your name on it?

Bethann21: Yes. I have and soon I will wire the travel agent the money.

Bethann21: Soon we will be with each other.

Andrew8613: Thank you my love I am so happy that you are taking care of this for me.

Bethann21: We will be together forever.

How SunTrust Protects You

You've put your trust in us and we want to let you know how we're safeguarding your accounts and identity.

We have several safety measures in place to help protect you, including industry-standard technologies on our Web site, and teams dedicated to fighting against fraud and identity theft.

Online Security at SunTrust

We realize that you, like many of our clients, rely on the Internet for your banking and financial needs. Following are some of the ways we ensure the online security of your personal and account information.

Secure Transmissions and Encryption: When you use the Internet to conduct transactions or communicate with us, it's critical that your information is handled securely. We use an encryption protocol called Secure Socket Layer (SSL) to protect your personal information. SSL converts sensitive data like passwords and personal identification numbers (PINs) into secure code and then sends them over a secure connection. Only SunTrust has the secret key that can decrypt your confidential information.

One way that you can tell your data is being protected is when you see a URL that begins with "https" (as opposed to "http"). Also, when you use the secure contact forms and email in Online Banking, your data is transmitted securely.

Firewalls: SunTrust computer networks are protected by firewalls. Firewalls prevent any unauthorized access to our computers and are one of the key safeguards that protect your information. Messages that do not meet our strict criteria are blocked by the firewall.

Virus Protection: We use the latest virus software programs on our systems to help us keep our computer networks virus-free. By using these programs, we ensure that you can communicate and transact with us in a safe and secure manner.

Email Policy

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.

At SunTrust, we have strict privacy policies in place. SunTrust will not trade, rent, or sell your personal information – including email addresses – to anyone. We will 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.html.

Third-Party Links: SunTrust may provide you with access to information, products, or services offered on nonaffiliated Web sites through the use of hyperlinks. By clicking on these links, you are directed from our Web site to a third-party site. SunTrust cannot guarantee how third-party Web sites collect information about you. SunTrust makes no representations or warranties regarding non-SunTrust sites or the companies maintaining them. If you choose to access non-SunTrust Web sites through links on our Web pages, we encourage you to review the privacy and security policies on those sites before you provide them with any personal or financial information.

Security Features: Our Products and Services

Whether you bank online or offline, our products and services have many built-in features that help protect your accounts and identity. From online security questions to Visa® Zero Liability, we have a number of safeguards in place to help protect your confidential information.

Online Banking Security Features

At SunTrust, convenience and security go hand-in-hand. Following are some of our Online Banking security features:

Automatic Sign-Off: SunTrust Online Banking automatically ends your session if there is no activity on your computer for 10 minutes. By automatically signing you out, the chances of unauthorized access to your accounts are minimized.

Unique User IDs and Passwords: Before you sign on to Online Banking, you need to enter a valid and unique Customer Identification Number (CIN)/User ID and Password. We recommend that your User ID and Password use a combination of letters and numbers so that they're difficult to guess.

Security Questions: When you sign up for Online Banking, we ask you to create security questions as part of your account profile. These security questions add an extra level of security to help prevent unauthorized access to your accounts.

Secure Email Correspondence: When you sign on to Online Banking, you are in a secure environment. This means that you can communicate with us via email safely and securely. To send us a secure email, visit suntrust.com, select the Online Banking link, and sign on with your CIN/User ID and Password. Then click Account Services and under Messages and Email, click Secure Message Center.

Online Statements: Online Banking allows you to access up to 18 months of your statements online. Online statements give you the power to closely monitor your accounts and quickly stop suspicious activities. You can also choose to stop having paper statements delivered to you and eliminate the chance of someone stealing them from your mailbox.

Online Bill Pay: Online Banking offers free Bill Pay that allows you to pay your bills securely and conveniently online. By paying your bills electronically, your personal and account information is securely transmitted and you decrease the chances of someone stealing your payments from your mailbox. Learn more about Bill Pay.

Direct Deposit: With Direct Deposit, your paycheck, Social Security, Supplemental Security Income benefits, or any periodic income is securely and directly transferred into your SunTrust account. Learn more about Direct Deposit.

Visa® Zero Liability: Visa Zero Liability is a feature we provide on all our credit and check cards. This feature protects you from unauthorized transactions. No matter where you shop, you'll never pay for transactions that you didn't authorize.

Verified by Visa®: Verified by Visa is a free service that protects your SunTrust Personal or Business Visa® Check Card from unauthorized use when you shop online. By registering for this service, you will receive a unique password that offers an extra level of security. You will be able to use this password at checkout on many retail Web sites. Learn more about Verified by Visa.

Online Banking Security Features

Identity Theft Protection and Credit Monitoring: At SunTrust, the protection of your identity and the security of your account information are important to us. That's why we've partnered with Equifax® to offer you special discounts on a simple, automated way to protect your credit through Equifax Credit Watch™ products.

With three levels of Equifax Credit Watch™ protection to choose from, you can select the product that works best for you. And because early detection is key – it's another way SunTrust helps to ensure the protection of your assets.

Equifax Credit Watch™ Silver is free¹ with select personal checking accounts and provides weekly monitoring with email and wireless alert options within seven days of any key changes in your credit file.

Equifax Credit Watch™ Gold and Equifax Credit Watch™ Gold 3-in-1 Monitoring are discounted premium monthly services which offer enhanced security features for SunTrust personal checking accounts, such as unlimited access to your Equifax Credit File and daily monitoring, with email and wireless alert options, within 24 hours of any key changes to your Equifax credit file.

To learn more about our partnership with Equifax and sign up for a Credit Watch™ product, visit suntrust.com/creditwatch.

You can also request your credit report from Experian at 888.397.3742 or experian.com or TransUnion at 800.680.7289 or transunion.com.

Our Security Policies and Processes

We use strict policies at SunTrust to protect your security. Following are some of our stringent processes that help protect your personal and account information.

Office and Branch Security: We have thousands of offices to conveniently serve you. Each of these locations uses industry-standard security methods, including alarms and monitoring systems, to protect our computers from unauthorized access.



¹ One free Equifax Credit Watch™ Silver subscription per Signature Advantage, Smart Solution Plus Checking, Preferred Checking, or Smart Solution Checking account. Additional Equifax Credit Watch products available at a discount to all checking account holders.

Visit the Web to Learn More About Scams

SunTrust Bank
suntrust.com

Federal Trade Commission
ftc.org

Federal Bureau of Investigation
fbi.gov/majcases/fraud/fraudschemes.htm

National Cyber Security Alliance
staysafeonline.info

National Fraud Information Center
fraud.org

Better Business Bureau
bbb.org

U.S. Department of Justice
internetfraud.usdoj.gov

U.S. Postal Inspection Service
usps.com/postalinspectors

The Internet Crime Complaint Center
ic3.gov

Joint Law Enforcement/Industry Task Force
lookstoogoodtobetrue.com



How To Contact Us

If you suspect suspicious or fraudulent activity with your SunTrust accounts, please report the incident to SunTrust.

By Phone

If you think you might be a victim of a scam:

- Call **800.SUNTRUST** (800.786.8787) seven days a week, 24 hours a day.
- You may also call the SunTrust Fraud Resolution Unit (available Mon. – Fri., 8:30 a.m. EST – 5:00 p.m. EST) directly at **866.493.3446**, *Option 2*.

Via Email

To report a suspicious email or pop-up Web page, forward information about the email or Web page to reportfraud@suntrust.com.

In Person

If you suspect you've been a victim of a scam and would like to discuss the matter in person, feel free to visit your nearest SunTrust branch.

To find a branch, visit suntrust.com and click ATM/branch locator at the bottom of the page to find maps, driving directions, and business hours to the SunTrust branch closest to you.

