



Protect Your Money and Identity

If criminals get your ATM, debit, or credit cards, or personal financial information such as account numbers, passwords, or Social Security number, they can drain your bank accounts or make charges to your credit cards. They may also commit a crime called identity theft by taking out loans and obtaining credits cards and even driver's licenses in your name.

There are 27 million victims of identity theft every year in the United States. Identity theft can seriously damage your credit and financial reputation, and it may take years to restore your good credit and name.

Don't let it happen to you! Here are tips to help you avoid financial fraud and safeguard your identity, bank accounts, and money:

About fraud and identity theft

- Identity fraud is usually limited to an isolated attempt to steal money from an existing account, such as a charge on a stolen credit card.
- With identity theft, a thief uses your personal information, such as your Social Security number or bank account number, to open accounts or initiate transactions your name. This may cause financial loss or damaged credit.
- If fraudulent transactions occur on your account, it does not automatically mean your identity was stolen. It may be an isolated incident of theft that can be quickly resolved. Contact your bank for more information.

Common ways ID theft happens

According to the Federal Trade Commission (FTC), skilled identity thieves use a variety of methods to steal your personal information, including:

1. Dumpster diving. They rummage through your trash looking for bills or other paper with your personal information on it.
2. Skimming. They steal credit/debit card numbers by using a special storage device when processing your card.
3. Phishing. They pretend to be financial institutions or companies and send spam or pop-up messages to get you to reveal your personal information.
4. Changing your address. They divert your billing statements to another location by completing a "change of address" form.
5. "Old-fashioned" stealing. They steal wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information. They steal personnel records from their employers, or bribe employees who have access.

Protect your money and identity (continued)

If you become a victim of identity theft:

- Contact your financial institution and credit card issuers immediately and alert them to the situation.
- Contact one of the three major credit bureaus and discuss whether you need to place a fraud alert on your file. This will help prevent thieves from opening a new account in your name.
- Here is the contact information for each bureau's fraud division:
 - Equifax 800-525-6285
 - Experian 888-397-3742
 - TransUnion 800-680-7289
- Close any accounts that have been tampered with or established fraudulently.
- File a report with law enforcement officials to help you with creditors who may want proof of the crime.
- Report all suspicious contacts to the Federal Trade Commission at www.consumer.gov/idtheft or by calling 1-877-IDTHEFT (438-4338).

General fraud prevention tips

- Carry only necessary information with you. Leave your Social Security card or unused credits cards at home in a safe and secure location.
- Protect your Social Security number. Don't write your Social Security number on a check. Give it out only if absolutely necessary or ask to use another identifier.
- Limit paper statements.
- Shred account statements or documents containing personal or financial information before discarding.
- Review your credit report at least once a year, looking for suspicious or unknown transactions.
- Limit the credit offers you receive.
- Remove your name from marketing lists.
- Never click on links sent in unsolicited emails; instead, type in a Web address you know.
- Keep your personal information in a secure place at home.

Card safety: ATM, debit and credit cards

- Report lost or stolen cards immediately to the company that issued you the card.
- To help you respond quickly in case your cards or ID are lost or stolen, make a chart like this one. Be sure to store the list in a safe place. Never carry it with you.

Credit card name	Financial institution	Account number	24-hour customer service #

Hands on Banking

Library Article: Protect Your Money and Identity

Card safety: ATM, debit and credit cards (continued)

- Sign your card on the signature panel as soon as you receive it.
- Protect your cards as if they were cash—never let them out of your possession or control.
- Do not include your card number in an email.
- Do not give out your card number over the phone unless you initiated the call.
- Be sure that you get your card back after every purchase.
- Don't leave your credit cards in your car's glove compartment. A high percentage of credit card thefts are from car glove compartments.
- Don't lend your cards—credit, debit, or ATM—to anyone. You are responsible for their use. Don't let your credit cards be used by others, even family and friends.
- Choose a PIN that is easy for you to remember but difficult for others to guess. Don't use any numbers or words that appear in your wallet (name, birth date, phone number, etc).
- Never tell anyone your PIN. No one from a financial institution, the police, or a merchant should ask for your PIN. You are the only person who needs to know it.
- Don't volunteer any personal information when you use your cards, other than by displaying personal identification as requested by a merchant.
- Never write down your personal identification number (PIN)—memorize it. Don't write down your account number and PIN and carry it with you. If your wallet or purse is stolen, someone else could have access to your money.
- When typing in your pin, cover the keypad so others can't see.
- When selecting a PIN, avoid picking a number that is easy for others to guess—for example, your name, telephone number, date of birth, or any simple combination of these.
- Always make sure that sales vouchers are for the correct purchase amount before you sign them.
- Always keep copies of your sales vouchers, credit card, and Automated Teller Machine (ATM) receipts.
- Always check your billing statement to make sure the purchase amounts are correct and to ensure there are no suspicious charges. Contact your service provider immediately if you see a charge you don't recognize.
- Always put disputes regarding your billing statements in writing immediately upon becoming aware of the disputed item; otherwise, you may be held legally responsible for the entire amount of the disputed item. Many credit card issuers have specific instructions for notifying them of a billing error dispute. Read your credit card agreement and billing statements carefully for information regarding dispute notification requirements. You may also contact your credit card issuer to ask about their dispute notification requirements.
- Shred or destroy your ATM receipts before you throw them away.
- Keep your cards away from magnets; these can erase the information stored on your card.
- If you receive a replacement card, destroy your old card. Destroy cards for cancelled accounts.
- Shop with merchants you know and trust. Make sure internet purchases are secured with encryption to protect your account information. Look for "secure transaction" symbols.

Protect your money and identity (continued)

ATM security tips

- Think about your personal safety when using an ATM. Because most ATMs give out cash and many accept deposits, it makes sense to be alert and aware of your surroundings no matter where or when you use an ATM. When you're by yourself, avoid using an ATM in out-of-the-way or deserted areas. Use ATMs located inside banks or supermarkets where other people are around. Use ATMs in well-lit, public areas.
- Be aware of your surroundings when withdrawing funds. If you notice anything out of the ordinary, come back later or use another ATM.
- If it looks like someone has tampered with the ATM equipment, don't use it. (This could mean that a criminal has attached a "skimmer" to the ATM to steal your financial information.) If a suspicious person offers to help you use the ATM, refuse and leave.
- When typing in your pin, cover the keypad so others can't see.
- After completing your transaction, remember to remove your card, cash and any printed documents such as receipts or statements.
- Put your money and ATM card away before you leave the ATM. Always avoid showing your cash. Always verify that the amount you withdrew or deposited matches the amount printed on your receipt.
- Take your receipts with you so potential criminals will not know how much you withdrew or how much money is in your account.
- When using a drive-up ATM, keep your car doors locked and your engine running.

Mail precautions

- If you stop receiving mail, call the post office immediately.
- Notify the post office immediately if you change your address.
- Get a mailbox that you must unlock with a key to remove your mail.
- Remove your incoming mail promptly.
- Don't leave your mail for long periods of time in visible, unguarded areas (e.g., apartment lobbies).
- If you're out of town, put a hold on your mail delivery or have a person you trust pick it up.
- Consider enrolling in an electronic payment service to reduce the risk of theft of your outgoing checks.
- Reduce your risk of mail fraud by replacing paper invoices, statements and checks with electronic versions, if offered by your employer, bank, utility provider or merchant.
- Review your statements both in paper and online to detect suspicious activity and fraud.
- Don't put outgoing mail in your residential mailbox. It could be stolen. Put outgoing mail in a secure USPS mail box or hand it directly to a uniformed USPS mail carrier.
- If you use the red flags found on some mailboxes to alert your mail carrier of outgoing mail, you are also alerting potential thieves that outgoing mail is in the box.

Hands on Banking

Library Article: Protect Your Money and Identity

Mail precautions (continued)

- Know your billing and statement cycles. If a company's regular bills or statements stop reaching you, contact that company immediately.
- Use an electronic bill pay service to help keep your information safe.
- If you stop receiving mail, call the post office immediately. Some criminals are able to forge your signature and have your mail forwarded elsewhere for the purpose of obtaining information that will allow them to apply for credit in your name.
- If you're told of a forwarding order placed on your mail without your knowledge, go to the post office to check the signature and cancel the order. Ask the post office to track down the forwarded mail—it can remain in the postal system for up to 14 days, so it may not yet have landed in the criminal's hands.

Bank account security tips

- Report lost or stolen checks immediately
- Review account statements carefully. Ask about suspicious charges.
- Enroll in online account statements if they're offered through your bank. Review them periodically for faster fraud detection.
- Limit the amount of information on checks. Don't print your driver's license number or Social Security Number on your checks.
- Store new and cancelled checks in a safe and secure location. Shred cancelled checks when you no longer need them.

Mobile banking security tips

- Frequently delete text messages with account balance information, and especially before loaning out, discarding, or selling your mobile device.
- Never disclose via text message any personal information (account numbers, passwords, etc.).
- Use the keypad lock or phone lock function on your mobile device when it is not in use. These functions password protect your device so that nobody else can use it or view your information.
- Store your device in a secure location.
- Let your bank know as soon as possible if you lose your mobile device or change your phone number.

Telephone safety

- Don't give your account number over the phone unless you initiated the call.
- When you purchase by phone, for maximum security, use a corded, rather than cordless phone.
- If you're contacted by a telephone salesperson (or "telemarketer"), ask questions. The fewer questions a telemarketer can answer, the less likely that it's a legitimate business. Write down the name, address, and phone number of the businesses or organizations that contact you. Ask for the names of other customers who can tell you about their experience with the business or organization.

Protect your money and identity (continued)

Online safety

- Keep your computer operating system up to date to ensure the highest level of protection.
- Use an up to date web browser.
- Install a personal firewall on your computer.
- Install, run, and keep anti-virus software updated.
- Avoid downloading programs from unknown sources.
- Never use your Social Security Number as your username to sign into online accounts.
- Never set your username to be the same as your password.
- Protect your online passwords. Don't write them down or share them with anyone.
- Use secure, encrypted web sites for transactions and shopping.
- Always log off from any banking, e-commerce or merchant web site. If you cannot log off, shut down your browser to prevent unauthorized access to your account information.
- Completely shut down your computer when you're not using it. Don't leave it in sleep mode.
- Don't send identifying personal information, such as account numbers, credit card numbers, or PINs via email. Financial institutions will never send you an email asking for this type of information.
- Select one credit card with a low credit limit to use for all your online purchases. Tell your credit card provider that you do not want them to raise the limit on this card without your prior written permission.
- Never download files or click on hyperlinks in emails from people or companies you don't know.

If someone's asking you to buy

- Unless you initiated the contact, never give out confidential information (such as account numbers, Social Security number, or mother's maiden name) to anyone.
- Be cautious when you receive offers to buy over the telephone, by mail, or on the Internet. Be especially careful about deals that sound too good to be true. Some of these offers may be illegal scams designed to cheat you. Don't respond to calls or emails requesting your account information to "award a prize" or "verify a statement."
- Beware of high-pressure sales people, especially if they tell you the sale must be made now.
- When in doubt, consult the Better Business Bureau or the U.S. Postal Inspection Service.

Home safety

- Be wary of strangers you allow into your home. Don't leave sensitive information, credit cards or checkbooks lying around.
- Store your new and cancelled checks securely.
- Keep your Social Security card in a secure place.

Hands on Banking

Library Article: Protect Your Money and Identity

Home Safety (continued)

- Photocopy your driver's license, credit cards, car registration, Social Security card and other identification, and keep the copies in a safe place.
- Shred unnecessary financial documents, old bank statements, invoices, and unwanted pre-approved credit offers. If possible, buy a shredder and mix the shredded paper thoroughly before throwing it out.

Monitor your financial activity

- Review your account statements as soon as you receive them. Notify the financial institution immediately if you notice errors or unauthorized activity.
- If your account statement is late in arriving, call your financial institution to find out why.
- Consider signing up for online banking. This will allow you to monitor your account activity at any time.
- Never tell anyone your online banking password and change it periodically.
- Check your credit report for accuracy at least twice a year. If a report lists unfamiliar accounts with large credit lines, you may be a victim of identity theft. Also review the "Inquiries" section of your reports. It tells you who has reviewed your credit history. If a car dealer in another part of the country has pulled your credit report, for example, you may be the victim of identity theft.

What is "phishing"?

- Phishing is usually a two-part scam involving email and spoof websites.
- Fraudsters, also known as phishers, send email to a wide audience that appears to come from a reputable company. This is known as a phish email.
- In the phish email are links to websites that spoof or imitate a reputable company's websites.
- Fraudsters hope to convince victims to give up their personal information by using clever and compelling language, such as an urgent need for you to update your information immediately.
- Once obtained, personal information can be used to steal money, or transfer stolen money into a different account.
- Fraudsters obtain email addresses from many places on the web. They also purchase email lists and sometimes guess email addresses.
- Fraudsters generally have no idea if people they send phish emails to are actual bank customers or not. They hope a percentage of the phish emails they send will be received by customers.
- A new form of fraudulent emails, called vishing or voicemail phishing, involves emails that contain fraudulent telephone numbers instead of links. Recipients of vishing emails are instructed to call this number and disclose personal and account information. Remember: always communicate with your bank by using a number you know to be associated with it, like the number found on the back of your debit card.

Protect your money and identity (continued)

Email & phish security tips

- Be wary of suspicious emails. Never open attachments, click on links, or respond to emails from suspicious or unknown senders.
- If you receive a suspicious email that you think is a phish email, do not respond or provide any information. Send the email to Anti-Phishing Working Group at reportphishing@antiphishing.org. Also, follow any phish email reporting procedures established by your bank.
- If you respond to a phish email with personal information, contact your bank immediately.

What is “skimming”?

- Skimming is a form of financial fraud where criminals copy the magnetic stripe encoding from your credit card using a hand-held device called a skimmer, which resembles an ATM keyboard. Each skimmer can hold data from hundreds of different credit cards.
- Once your credit card has been swiped through the device, the thief has the information needed to make a counterfeit card.
- Thieves often sell the data to other people. The data can be downloaded into a computer and emailed anywhere around the world and is used to make counterfeit credit cards.
- Monitor your credit card statements carefully and report any unauthorized activity immediately.

About Scams

- Fraudsters try to contact and defraud potential victims using various means. Once they contact potential victims, they use compelling language and scenarios to scam them.
- If you're involved in a situation that matches one of the following descriptions, it could be a scam and you should contact your bank immediately:
 - **Job scams:** You are paid or receive a commission to facilitate money transfers through your account or apply for a job that asks you to set up a new bank account.
 - **Dating scams:** Someone you met through an online dating site or chat room asks you to send money for a variety of reasons including a need for urgent surgery or to make travel arrangements to meet in person.
 - **Lottery or sweepstakes scams:** You receive notice that you are the winner of a lottery that you did not enter, but must pay a small percentage for alleged taxes or other fees before you can receive the rest of your prize.
 - **Internet scams:** You receive a check for something you sold over the internet, but the amount of the check is more than the selling price. You are instructed to deposit the check, but send back the difference in cash.
 - OR** You receive a check from a business or individual different from the person buying your item or product.
 - OR** You are instructed to transfer money, or receive a transfer of money, as soon as possible.
- Remember, if it sounds too good to be true, it probably is.

Hands on Banking

Library Article: Protect Your Money and Identity

Scam prevention tips

- Don't accept payments for more than the amount of the service with the understanding that you send them the difference.
- Don't accept checks from people you've only met online.
- Don't accept jobs in which you are paid or receive commission for facilitating money transfers through your account.
- Be wary of job offers that require you set up a new bank account.
- You are ultimately responsible and liable for all deposits made into your account, whether they are a check, money order, transfer, etc.
- Don't accept payments for more than the amount of the service with the understanding that you send them the difference.
- Don't accept checks from people you've only met online.
- Don't accept jobs in which you are paid or receive commission for facilitating money transfers through your account.
- Be wary of job offers that require you set up a new bank account.
- You are ultimately responsible and liable for all deposits made into your account, whether they are a check, money order, transfer, etc.

We invite you to contact Wells Fargo for further information and assistance. Visit our Web site at wellsfargo.com or any Wells Fargo store.