



Call us at 866-232-9890

Privacy & Security

Send us an email

Charles Schwab & Co., Inc.



Privacy & Security

[Schwab's Privacy Policy](#)

[Online Privacy & Information Security](#)

[Identity Theft Prevention Program](#)

[View Schwab Bank privacy and security practices](#)

Schwab's Privacy Policy - A Commitment to Your Privacy (Effective July 2, 2007)

At Charles Schwab & Co., Inc. ("Schwab") our most important asset is our relationship with you. We are honored that you have entrusted us with your financial affairs, and we are committed to safeguarding the privacy of information we maintain about you. Establishing and adhering to an effective privacy policy is an important part of that dedication.

Below, you will find details about Schwab's commitment to protecting your privacy, including the types of information we collect about you, how we use and share that information both within and outside the Schwab family of companies, and how you can instruct us to limit certain types of information sharing.

Our privacy policy applies to all clients with whom we have a relationship and is also extended to each of our former clients.

Your Privacy Is Not for Sale

Simply put, we do not and will not sell your personal information to anyone, for any reason, at any time.

How We Collect Information About You

We collect personal information about you in a number of ways.

- **Application and registration information.**

We collect information from you when you open an account or enroll in one of our services. You will also be asked for information when you choose to participate in a Schwab promotion. We may also collect information from consumer reporting agencies to verify your identity in the account-opening process or if you apply for a margin account. The information we collect may include your name, address, phone number, email address, Social Security number and date of birth, as well as details about your interests, investments and investment experience.

- **Transaction and experience information.**

Once you have opened an account with us, we collect and maintain personal information about your account activity, including your transactions, balances, positions and history. This information allows us to administer your account and provide the services you have requested.

- **Third-party information providers.**

We may collect information about you from information services and consumer reporting agencies to verify your identity, employment or creditworthiness, or to better understand your financial needs.

- **Website usage.**

When you visit our website, our computer may use devices known as "cookies," graphic interchange format files (GIFs), or other similar Web tools to enhance your Web experience. These tools enable us to recognize you when you return to our site, maintain your Web session while you browse, as well as help us provide you with a better, more personalized experience at Schwab. To learn more about our policies regarding using our Website and the use of web tools, please visit Online Privacy and Security.

How We Share Information About You Within the Schwab Family of Companies

Charles Schwab & Co., Inc. is part of the Schwab family of financial services companies that are owned by our parent, The Charles Schwab Corporation. These companies are often referred to as "affiliates" and include, but are not limited to:

The Charles Schwab Corporation

Charles Schwab & Co., Inc., a broker-dealer
Charles Schwab Bank, N.A., a retail bank
CyberTrader, Inc., a broker-dealer for active traders

Many clients within the Schwab family of companies do business with more than one affiliate, creating an efficient, comprehensive financial relationship to meet individual needs. When appropriate, Schwab may share information we collect about you within our family of companies to:

- help provide you with better service or perform services on our behalf;
- respond to communications from you or as you authorize or request;
- make it more convenient for you to open a new account;
- allow an affiliate to provide you with information about its products and services that we believe may benefit or interest you.

You may instruct us **not** to share information about you with our affiliates for certain purposes, as explained under "How to Limit the Sharing of Information About You."

How We Share Information About You Outside of the Schwab Family of Companies

We provide access to information about you to outside companies and other third parties in certain limited circumstances, including:

- to help us process transactions for your account;
- when we use another company to provide services for us, such as printing and mailing your account statements;
- when we believe that disclosure is required or permitted under law. For example, we may be required to disclose personal information to cooperate with regulatory or law enforcement authorities, to resolve consumer disputes, to perform credit/authentication checks, or for risk control;
- when we enter into a joint marketing agreement with another financial institution in order to provide you with a Charles Schwab & Co.-branded (or other Schwab affiliate-branded) financial product or service. We only make such agreements with companies that we believe can help us provide a financial product or service that will benefit you.

You may instruct us **not** to share information about you with outside companies for joint marketing purposes, as explained under "How to Limit the Sharing of Information About You."

How to Limit the Sharing of Information About You

If you prefer, you may choose to limit the information we share about you with our affiliates and outside companies. Specifically, you may instruct us:

- **not** to share with our affiliates consumer reports and other personal information about you that may be used to determine your eligibility for credit (for example, information about your income, profession or employment status);
- **not** to allow our affiliates to market their financial products or services to you based on information they receive from us about your eligibility for credit or your transactions and experiences with us;
- **not** to share personal information about you with an outside company for joint marketing purposes.
- You may exercise this choice by calling us at **877-812-1817**; or
for services in Chinese at **800-662-6068**;
for services in Spanish at **800-786-5174**;
from outside the U.S. at **415-667-5009**;
- Your choice will be applied to you as an individual and will automatically be extended to all of your accounts with us, as well as to any accounts you may have with any of our affiliates.
- Joint account holders may instruct us on behalf of another account holder.
- You may make your privacy choice at any time and it will remain in effect until you change it.

If you choose to limit these types of information sharing, we may continue to share information with our affiliates that identifies you (such as your name and Social Security number), as well as information about your transactions and experiences with us. In addition, our affiliates may continue to use information they receive from us to perform services on our behalf, to respond to communications from you, as you authorize or request, or, if you are their customer, to offer you products or services. We may also continue to share information about you with outside companies as permitted or required by law.

State Laws

We will comply with state laws that apply to the disclosure or use of information about you. For example, if your address is in Vermont, we will automatically limit information sharing as described in "How to Limit the Sharing of Information About You" without your having to advise us of this privacy choice.

The following notice is required to be made under Nevada law to all customers with a Nevada mailing address. At any time, you may

request to be placed on our internal “do not call” list. You may do so by calling Schwab at **800-435-4000**. Customers from any state may request to be placed on Schwab’s internal “do not call” list by calling **800-435-4000**. If you would like further information about this notice, you may contact us at Charles Schwab & Co., Inc., 101 Montgomery Street, San Francisco, CA 94104; or call **800-435-4000**. For services in Chinese, please call **800-662-6068**. For services in Spanish, please call **800-786-5174**. From outside the U.S., please call **415-667-5009**. Email us at Privacy@schwab.com. For more information about the Nevada “do not call” notice requirement, you may also contact the Nevada Attorney General, 555 E. Washington St., Suite 3900, Las Vegas, NV 89101; phone: **702-486-3132**; email: BCPINFO@ag.state.nv.us.

Safeguarding Your Information, Maintaining Your Trust

We take precautions to ensure the information we collect about you is protected and is accessed only by authorized individuals or organizations.

Companies we use to provide support services are not allowed to use information about our clients for their own purposes and are contractually obligated to maintain strict confidentiality. We limit their use of information to the performance of the specific services we have requested.

We restrict access to personal information by our employees and agents. Our employees are trained about privacy and are required to safeguard personal information.

We maintain physical, electronic and procedural safeguards to protect personal information.

Teaming Up Against Identity Theft

Identity theft is a serious concern to all of us. Safeguarding information to help protect you from identity theft is our priority. Schwab takes steps to protect you from identity theft by:

- utilizing client identification and authentication procedures before initiating transactions;
- creating a secure transmission connection to our Schwab websites. You will see the padlock in the lower right corner of your browser's frame indicating it is a secure site;
- ensuring our employees are trained to safeguard personal information about you.

You can also help protect your identity and accounts. Here are a few steps to remember:

- Schwab will never request your account number, login password, or Social Security number in either a non-secure or unsolicited email communication;
- shred documents that contain personal information;
- check your credit report regularly for unauthorized activity and protect your personal identification numbers (PINs) or personal data.

If you have been a victim of identity theft or to learn more about protecting yourself against identity theft, go to the [Identity Theft Prevention Program](#).

Greater Accuracy Means Better Protection

We are committed to keeping accurate, up-to-date records to help ensure the integrity of the information we maintain about you. If you identify an inaccuracy in this information, or if you need to make a change to it, please contact us promptly by calling **800-435-4000**.

A Commitment to Keeping You Informed

We will provide you with advance notice of important changes to our information-sharing practices.

Contact Us with Questions

If you have any questions or concerns, please contact us by email at Privacy@schwab.com or call us at **800-435-4000**.

For services in Chinese, please call **800-662-6068**.

For services in Spanish, please call **800-786-5174**.

From outside the U.S., please call **415-667-5009**.

[Return to top](#)

Online Privacy and Information Security

If you have a security-related concern, please call us at **888-3-SCHWAB**. We will work closely with you to ensure a rapid and personal response to your concerns.

Schwab understands that you have entrusted us with personal information that is both important and confidential. We take our responsibility to protect your information extremely seriously.

Schwab updates its security and privacy standards to guard against identity theft and provide security for your account information. We constantly re-evaluate our security and privacy policies and adapt them as necessary to deal with new challenges.

Schwab's account protection efforts fall into but are not limited to these categories:

1. Authentication – Secure identification and authentication before initiating transactions
We maintain strict rules for the creation of secure user IDs and passwords, designed to stop others from guessing your log in information.
2. Web site Security – Secure transmission connection to our Schwab Web sites
We use Secure Sockets Layer (SSL) technology and encrypted “cookies” to establish and maintain a secure transmission connection and encrypt data passing between your computer and our systems. This is designed to prevent anyone from intercepting or viewing your personal information.
3. Email Security – Policies to fight “phishing” and other email-related security challenges
Schwab is constantly re-assessing its email security and log in standards to provide protection against new and changing security challenges.
4. Transaction Monitoring, Employee Oversight and Access Control – Watching for unusual account behavior
We have highly sophisticated internal transaction monitoring systems in place to identify potentially suspicious and fraudulent activities. These systems are combined with strict controls on employee access to account information, creating a further layer of protection for your information.
5. Training – Employee training
Schwab employees are trained to safeguard your personal information.
6. Steps you should take
You play an important role in safeguarding your personal information and protecting your privacy. Here are some of the things you can do.
7. The Schwab Security Guarantee

More information on our security measures can be found below.

Authentication

Authentication is the process that our clients go through to access secure areas of our Website. This process takes place when you log into your account. The two key components of login are your Login ID and Password.

Login ID: We urge you to create your own unique Login ID and recommend that it be a Login ID that you don't commonly use for other purposes. We particularly urge you not to use your Social Security or number date of birth as a Login ID. Please call Schwab at **800-435-4000** and a representative will assist you in creating a new Login ID.

Passwords: We maintain strict rules to help prevent others from guessing your password, and recommend that you change your password periodically. Your password must meet the following criteria:

- 6-8 characters long
- Include both letters and numbers
- Include at least one number between the first and last character

In addition, for your protection, repeated unsuccessful attempts to log in will cause your online access to be disabled. Once this happens your password must be reset. If this happens to you inadvertently, please follow the instructions under “Forgot your password” on the Login page






[Return to top](#)

Web Site Security

From the time you submit your Login ID and Password, communications between your computer and Schwab are encrypted using Secure Sockets Layer (SSL3) technology, a secure communication protocol that protects your privacy. SSL enables client and server applications to communicate in a way that is designed to prevent eavesdropping, tampering and message forgery.

To support this technology, you need a recent version of an SSL3-capable, 128-bit browser, such as Netscape, Microsoft Internet Explorer, or AOL. These browsers will activate SSL3 automatically whenever you sign on to your Schwab account.

Look for the padlock! To ensure that SSL encryption is protecting your private communications, look for a small picture of a padlock on the browser frame. Another indicator is the URL prefix “HTTPS”. See below.

<p>HTTPS indicator Located in the URL address in all browsers.</p>	
<p>Internet Explorer The padlock appears in the lower right corner of the browser frame.</p>	
<p>Mozilla Firefox The padlock appears to the right of URL in the address bar as well as in the lower frame of the browser</p>	
<p>Apple Safari The padlock appears in the upper right hand corner of the browser frame.</p>	
<p>Netscape The padlock appears in the lower right hand corner of the browser frame.</p>	

If you move the cursor over the “locked padlock” icon, a pop-up message will appear stating “SSL Secured (128 Bit).” Absence of the pop-up message may indicate that you are connected to a “phishing site.”

Another important information security measure in place throughout Schwab’s Web sites is the timeout feature. This feature will log you out of your account if there has been no activity within a specified amount of time. It is designed to stop others from accessing your account if you fail to log out.

We have implemented these measures for your protection, but you should still remember to log out each time you have finished accessing your Schwab accounts.

Branch Kiosks:

Schwab maintains particularly strong information security controls at the computer kiosks in its nationwide branch network to protect your account data. These measures include:

- A highly controlled environment with limits on the Web sites clients are allowed to visit, the applications they are allowed to open, the Internet technologies they are allowed to use, and the operating system controls they are permitted to access.
- Additional and more aggressive timeout policies that go beyond the timeout policies on our Web site. These will log you out of your account automatically if you walk away from the kiosk without logging out. The quick timeouts are based on keyboard activity and infrared sensors that detect when you have physically moved away from the kiosk. We have implemented these measures for your protection, but you should still remember to log out each time you have finished accessing your Schwab accounts

Cookies:

Cookies enable us to understand better how you and others use Schwab's online channels. They allow us to collect information about where your browser goes on our Web sites. This assists us in understanding your preferences and improving our Web site. For example, the information we obtain from cookies or GIFs (Graphical Interchange Format) helps us understand whether our customers use certain Web features and how to improve navigation. We also may use information gathered as the result of GIFs or cookies to target emails or Web messages. Knowing where your browser has been on our website helps us present useful information and offers to you. We do not sell this or any other information about you to other websites, merchants or financial institutions. Unless you have affirmatively consented, we do not provide any personally identifiable information about you to anyone else for their marketing purposes.

Cookies come in two flavors: persistent and session-based.

- Persistent cookies remain on your computer after you've closed your browser or turned off your computer. They include a unique identifier for your browser that only Schwab can read and use, and that tells us you are a Schwab customer or prior Schwab Web site visitor. We are especially careful about the security and confidentiality of the information we send through persistent cookies. For example, we do not store account numbers or passwords in persistent cookies.
- Session cookies exist only during an online session with Schwab. They disappear from your computer when you close your browser software or turn off your computer. Session cookies allow you to conduct transactions or request your own personal or account information on our Web site. They contain encrypted or encoded information about your account(s), and/or identifying information that you have previously provided to us. This information allows Schwab to process your online transactions and requests

[Return to top](#)

Email Security

Recently there has been rapid growth in email-related information security challenges such as “phishing” or “spoofing” schemes. These fraudulent techniques attempt to fool you into giving up your personal data by impersonating legitimate communications from financial service providers. We are working with other financial institutions and technology leaders to prevent these security challenges from impacting our clients. Measures currently in place or underway include:

- Implementation of domain-verification technologies that, in cooperation with Internet service providers, will enable clients to verify that emails claiming to have come from Schwab actually did come from Schwab.
- Standardization of Schwab emails and adherence to industry anti-phishing best practices. We continually re-design our email policies to incorporate the latest tools and standards aimed at preventing phishing.
- Ongoing assessment and implementation of new login technologies designed to prevent others from masquerading as our Web site.

[Return to top](#)

Transaction Monitoring, Employee Oversight and Access Control

We use automated transactional monitoring tools to detect suspicious account activity. When these sophisticated systems flag a questionable transaction we contact the client to be sure the transaction is legitimate and that it will be processed safely and rapidly. This combination of automated and manual transaction monitoring further strengthens the security we provide for your financial and personal information.

[Return to top](#)

Employee Training

Training:

We take precautions to ensure that your account and personal information at Schwab are accessed only by employees who are authorized and monitored. This is done through access controls and training, as well as physical, electronic and procedural safeguards. Employees are trained in our notifications policy and are required to promptly report any potential breach to our swift response team. All customers are covered by Schwab's Breach Notification Policy. In July 2003, Schwab implemented a corporate policy on breach notifications and a centralized swift response team was established. Privacy, Risk Management & Investigations, Information Security, Legal, Corporate Communications and other of our business units work together to respond to potential incidents as quickly as possible.

- All customers are covered by Schwab's Breach Notification Policy. In July 2003, Schwab implemented a corporate policy on breach notifications and a centralized swift response team was established. Privacy, Risk Management & Investigations, Information Security, Legal, Corporate Communications and other of our business units work together to respond to potential incidents as quickly as possible.
- Potential incidents are tracked, assessed and investigated. When necessary outside law enforcement agencies become involved.

[Return to top](#)

Steps you should take

Client Security Practices

Your participation is an important component of all of our security efforts. We believe it is essential that we work in close cooperation with you as our client to maintain the highest levels of security. These are the steps you should take to protect your account:

Protecting the security of your computer

- Keep your computer and browser software current with security updates.
- Install and update anti-virus and anti-spyware software and use personal firewalls to protect your computer.
- Be alert to the threats posed by malware--short for malicious software, this form of software is designed specifically to damage or disrupt a system, or to secretly record information such as keystrokes. Malware types include key logging tools, trojan horses, hijacking programs, and dialer programs that may reside on your personal computer. While these threats constantly evolve, you can help protect your personal information and computer by using a personal firewall, maintaining up-to-date anti-spyware and anti-virus programs, and by immediately reporting any suspicious activity involving your personal information.
- Do not enable any application features that would automatically log you in to your Schwab account or pre-fill the Login ID or Password fields.
- Change your password periodically and avoid using passwords for Schwab that you commonly use for other purposes.
- For more information on how to protect your personal computer, including links to vendors providing anti-virus and anti-spyware software, please visit the Federal Trade Commission's computer security site at <http://onguardonline.gov>. Microsoft Corporation provides additional information specific to the Windows operating system at <http://www.microsoft.com/security>. Users of Apple computers can find security information at <http://www.apple.com/support/security>.

Using your computer

- Your username and password are for your use only. Do not share them with anyone.
- Check to make sure you are interacting with a secure Web site [see above](#).
- Always log off after accessing your Schwab account. This prevents someone else from accessing your account if you leave your computer unattended while the session has not yet "timed out," or automatically shut down.
- Be careful about using [third-party computers](#) or computers that you are not familiar with, such as those in Internet cafés.

If you do use a third-party computer, be particularly careful to ensure you have fully logged out. Schwab's systems are set to prevent browsers from saving account information in a computer's Internet cache, but as an extra precaution you may want to clear the cache of any public computer on which you have accessed your Schwab accounts. Please check the browser's help section to learn how to manually clear its Internet cache.

Reading your statements:

- Review your account statements carefully.
- Reduce the risk of lost and stolen paper statements by subscribing to online account statements and confirmations. You can sign up for paperless products quickly and easily by going to www.schwab.com/paperless.

Recognizing and fighting fraud

- Do not provide personal or financial information in response to an email request or by clicking on a link, unless you are able to verify the authenticity of the site to which you are taken through the SSL padlock or other means.
- Do not enter personal information into a form within an email message or a pop-up.
- Note that Schwab will never ask you to provide personal financial information in an email.
- Do not open an email from a sender that you do not recognize. Be particularly cautious of any attachments to emails from unrecognized sources.
- Immediately report any unusual activity regarding your Schwab accounts to our representatives at **888-3-SCHWAB**.

[Return to top](#)

Identity Theft Prevention Program

[How Schwab Protects Your Identity](#)

[How to Protect Against Phishing](#)

[What to do if You Are A Victim of Identity Theft](#)

[Other Resources to Learn More about ID theft](#)

How Schwab Protects Your Identity

Your privacy is our priority and Schwab is committed to protecting you

- We do not sell customer information to anyone.
- We use encryption technology to protect sensitive information that is transmitted over the Internet.

- We control access to your information inside our company by limiting employee access to systems and data.
- We ensure all employees are trained to safeguard your information.
- We continue to evaluate our efforts to protect personal information and make every effort to keep your personal information accurate.

Our most important asset is our relationship with you. We understand that you have entrusted us with your private financial information, and we do everything we can to maintain that trust.

[Return to Top](#)

How to Protect Against Phishing

What Is Phishing?

Phishing is the illegal attempt to mislead consumers into providing personal or financial information, including account numbers, passwords and Social Security numbers, via email or through fraudulent Web sites.

The most frequent phishing attacks occur through email disguised to appear as though it came from a reputable financial institution or company.

Most phishing attempts urge you to update or validate your account information, typically through a link in an email directing you to a fake Web site that appears to be legitimate.

How To Spot a Phishing Attack

There are many phishing attacks active on the Internet. Here are a few of their lines and lures:

- An email contains an “urgent” or “shocking” tone requesting your immediate action on an account-related matter. Phishers frequently succeed by getting consumers to act quickly without thinking.
- An email is sent from a user falsely claiming to be a legitimate company with an attachment. An unsolicited email attachment more than likely contains a virus. Do not open it.
- A pop-up window appears from a user falsely claiming to be a legitimate company’s Web site asking for personal information.

Learn More About Phishing Scams or Identity Theft

Additional information can be found at www.antiphishing.org or www.consumer.gov/idtheft/.

How To Report a Phishing Attack

If you suspect you have received a fraudulent email from The Charles Schwab Corp. or any of its subsidiary companies, please contact: Privacy@schwab.com. If you believe that any communications with or from Schwab resulted in identity theft, call us immediately at **800-435-4000**.

[Return to Top](#)

What To Do If You Are A Victim of Identity Theft

If you are a victim of identity theft, here are some recommended steps:

- Contact Schwab and let us know you have been a victim of identity theft
- Contact the fraud departments of each of the 3 major credit bureaus:

	Equifax	Experian	Trans Union
Report Fraud	800-525-6285	888-397-3742	800-680-7289
Order Credit Report	800-525-6285	888-397-3742	800-916-8800
Web address	www.equifax.com	www.experian.com	www.transunion.com
Address	PO Box 740241 Atlanta, GA 30374-0241	PO Box 9530 Allen, TX 75013	PO Box 6790 Fullerton, CA 92634-6790

- **Report the identity theft and request a "fraud alert."** This ensures that you will be contacted before any new account is opened and/or an existing account is changed.
- **Request copies of credit reports.** Review the reports carefully and identify any new accounts that may have been opened. Pay particular attention to the section of the report that lists "inquiries" from new companies. Contact these companies immediately and have them remove any pending or new accounts from their system. **Note: Credit bureaus must provide free copies of credit reports to victims of identity theft. Contact the fraud departments of creditors to dispute unauthorized charges (e.g., credit card issuer, phone companies, utilities, banks, other lenders.) Describe your identity theft problem and follow up with a letter.**

- **Contact the fraud departments of creditors to dispute unauthorized charges** (e.g., credit card issuer, phone companies, utilities, banks, other lenders.) Describe your identity theft problem and follow up with a letter.
- **File a report with your local police department and ask to file a report.** This may help when clearing your credit.
- **File a complaint with the Federal Trade Commission (FTC).** The FTC handles complaints from victims of identity theft, provides information to those victims, and refers complaints to appropriate entities, including the major credit-reporting agencies and law enforcement agencies.
- By Phone: **877-ID THEFT**
- Online Complaint Form: www.consumer.govidtheft

Other Resources to Learn More about Identity Theft:

Federal Trade Commission - Internet Fraud -- www.onguardonline.gov

Federal Trade Commission - IDTheft -- www.ftc.gov/bcp/online/pubs/credit/idtheft.htm

Federal Trade Commission - Phishing -- www.ftc.gov/bcp/online/pubs/alerts/phishingalrt.htm

Identity Theft Resource center -- www.privacyrights.org

Identity Theft Prevention and Survival -- www.identitytheft.org

Social Security Administration -- www.ssa.gov/oig/guidelin.htm

Justice Department -- www.usdoj.gov/criminal/fraud/idtheft.html

Postal Inspection Service -- www.usps.com/websites/depart/inspect

Please note, these links are being provided as a service convenience. Schwab is not affiliated with any of these organizations and cannot guarantee their accuracy, effectiveness and/or completeness.

[Return to Top](#)

Brokerage Products: Not FDIC Insured • No Bank Guarantee • May Lose Value

[Home](#) | [Contact Us](#) | [About Schwab](#) | [Site Map](#) | [Privacy & Security](#) ©2007 Charles Schwab & Co, Inc. All rights reserved. Member SIPC