Protect your computer and network

Protect your computer against new viruses or other attacks with anti-virus and anti-spyware software, and configure all software for automatic updates. The anti-virus and anti-spyware software included in operating systems require frequent updates to keep pace with new risks. Security software included with new computers generally require a subscription for protection to continue. Need to upgrade your security products?

Use the latest version of your web browser. Strong encryption protects your information as it travels over the Internet. Older web browsers may not support the highest strength 128-bit encryption.

Do not allow software to be loaded on your computer if you're not completely familiar with it. If you share your PC with anyone, including your children, make sure they know the rules for downloading and installing software.

Install a hardware- or software-based firewall. A firewall controls how information moves between a computer and a network to help ensure that only legitimate traffic takes place, and hides the presence of computers behind it to make it more difficult for potential intruders to find them.

Create secure passwords

Choosing your password well and keeping it a secret can be key steps to safeguarding all of your online transactions. To create a password that is more difficult to guess, use a combination of letters and numbers for passwords you create (i.e. 4funcallC3po, Il9vemyd1g). Certain passwords are easier to compromise, so try to avoid common pitfalls by creating secure passwords:

- **Don't base your password on personal information**—such as the name of your pet or your company.
- **Don't use a word found in the dictionary as your password.**
- **Avoid substituting numbers for letters**, for example: using a zero for the letter "o" or a one for the letter "i." These substitutions are well known and predictable.
- **Don't use your UserID** as your password.
- **Don't use simple number sequences** like "12345" or a series of duplicate numbers like "11111."
- **Change your password frequently**, and don't "recycle" a password you've used somewhere else.

Know the threats

It's important to be aware of possible risks to your computer and the information on or passing through it. We have a designated team responsible for reviewing potential threats to clients' assets and information.

Your awareness, combined with our vigilance, can help to decrease the risk to your accounts and information.

Familiarize yourself with the threats posed by:

- Identity theft
- Phishing
- Stock spam
- Spyware
- Viruses, worms, and Trojans

Identity theft

Identity theft—using a person's personal or financial data to commit fraud—is one of the most rapidly growing global crimes. The targets of this crime are personal information, financial information, and access to online accounts.

The personal information often targeted includes:

- Name, address, and date of birth
- Social Security number
- Driver's license number
- Passport
- Signature

The financial information often sought is:

- UserIDs and passwords
- Account numbers and ABA numbers
- Credit card numbers
- ATM / Debit cards
- Checks

Phishing

Phishing is when someone attempts to steal personal or financial information. It usually starts with an email asking for sensitive information, such as your UserID or user name, your password, or your account information.

Phishing—sometimes also referred to as **pharming**—opens the door to identity theft and computer security breaches.

Please note: We will never ask you for your account number, UserID, PIN, password or any other personal information in an email. (In rare cases, however, we might need to ask you for the last four digits of your account number for identification purposes.)

Spyware

As its name suggests, spyware is software that is used to "spy" on your computer. It poses two problems: invasion of privacy and can adversely affect your computer's performance.

Viruses, worms, and Trojans

Viruses, worms and Trojan horses (often referred to as just Trojans) are programs that can become embedded on your hard drive. They can allow remote access to your computer, send spam, be used to spy on you, log your keystrokes, aid phishers, erase data, and even wipe out your hard drive.

- A virus is computer code that infects your computer when you take a certain action, such as double clicking on an email attachment. A virus typically embeds in your existing software and uses it to reproduce and spread.
- Unlike viruses, worms are stand-alone programs. They do not embed themselves into another piece of software, but spread by duplicating themselves without any intervention from you.
- A Trojan is a stand-alone program that spreads by masquerading as a harmless file or program and tricking the user into installing it on his or her machine. Many Trojans arrive under the guise of a picture, screensaver, or email attachment. Once a user opens the file, the Trojan installs itself on the computer and may take over the computer's email program or use its own email program for malicious purposes.

 The Asset Protection Guarantee

If you lose cash or securities from your account due to unauthorized activity, we'll reimburse you for the cash or shares of securities you lost. We're promising you this protection, which adds to the provisions that already govern your account, if unauthorized activity ever occurs and we determine it was through no fault of your own. Of course, unauthorized activity does not include actions or transactions undertaken by or at the request of you, your investment advisors or family members, or anyone else whom you have allowed access to your account or to your account information for any purpose, such as trading securities, writing checks or making withdrawals or transfers.

We promise this protection if you work with us in four ways:

1. Keep your personal identifying information and account information secure and confidential because sharing your UserID, password, PIN, account number or other standard means of authentication with other people means you authorize them to take action in your account.
2. Keep your contact information up-to-date with us, so that we can contact you in case of suspected fraud.
3. Review your account frequently and your statements promptly and report any suspicious or unauthorized activity to us immediately in accordance with your Client Agreement.
4. Take the actions we request if your account is ever compromised and cooperate with our investigation.

If you help us protect you in these basic ways, we'll promise no fine print and no footnotes — just our commitment to protect the assets you entrust to us.

What is the Asset Protection Guarantee

What is the asset protection guarantee?

This guarantee means that if you lose cash or securities from your account due to unauthorized activity through no fault of your own, we'll reimburse you for the cash or shares of securities you lost out of your account.

To provide this guarantee, we ask you to help us help protect your assets and information in the following simple ways:

- Keep your account access information private: Don't write it down near your computer, let a neighbor or co-worker watch you type in a UserID or password, or give login information to anyone you don't want to gain access to your account. Remember that any individuals you've granted authority to act on your behalf in your account (perhaps your spouse, child, or

investment advisor) would be considered authorized, so their activity isn't covered by this guarantee.

- Check your account frequently.
- Carefully review your account statements and trade confirmations.
- If you ever suspect that you've been a victim of theft or that unauthorized activity has occurred in your account, please notify us immediately. We'll investigate your claim promptly. We'll help you take steps to protect yourself and your system from further loss. We'll also ask you to cooperate in any investigation that might be necessary.

We're committed to delivering one of the highest levels of security in the industry and safeguarding your privacy. Our firm is carefully managed under intensive regulatory oversight and following strict security requirements. We continually review our security practices. All of these measures are our ultimate insurance for our clients' assets; this guarantee protects you in the unlikely event that your assets are stolen.