



Online security: Our promise to you

Clients like you make Vanguard special. The security of your information is extremely important to us, so our commitment to you is simple:

We'll reimburse you the amount taken from your Vanguard account in an **unauthorized** online transaction on vanguard.com if you've followed the steps described in the **Your responsibilities** section below.

Your responsibilities

You should be aware of the risks of sharing your account information: If you share your vanguard.com user name and password, or if you allow someone to access your account information, activities performed with your shared or accessed credentials or information may be considered **authorized**. If you've given someone authority to transact on your behalf, that person's activity is **authorized**.

Need technical assistance?

Contact Web Technical Support Services at 888-353-0547, Monday through Friday, 8 a.m. to 7 p.m., Eastern time.

Report security concerns

Receive a suspicious email claiming to be from or about Vanguard? Forward it to us at phish@vanguard.com.

Have other security concerns? Email us at abuse@vanguard.com.

Remember that everyone has a role to play in account security. Here's how to do your part.

Protect your computer/device.

- Make sure that any computer or device you use to access your accounts has up-to-date antivirus and antispyware software and is protected by a firewall.
- Don't use a public computer unless you know it has up-to-date security and you can log off completely.

Protect your vanguard.com user name, password, and other account-related information.

- Make sure your user name, your password, and the answers to your security questions are unique and strong, and keep them secure.
- Be careful about responding to, opening attachments in, or clicking links in emails that ask you for personal or financial information, because you may expose account-related information. Vanguard will never send you an email asking for your Social Security number, account numbers, passwords, or security questions and answers.
- Don't store your password or answers to security questions on the computer or device you use to access your Vanguard accounts.

Monitor the activity in your account, and alert us immediately of any activity you didn't authorize.

- Review the account-related information we send or make available to you as soon as you receive it, such as account statements, confirmations, and changes to your mail preferences (such as an address change), bank information (such as the addition or deletion of a bank), and other services.
- Let us know immediately if you discover unauthorized activity, whether that activity is a transaction, a change to your account, or the addition, removal, or change of an account option or service. If you see something that you don't understand or that looks unusual, contact us for an explanation.

Cooperate with us.

If Vanguard investigates suspected unauthorized activity in your account, you must fully cooperate with us. For example, we may ask you to file a police report, provide us with a statement of facts, or allow us access to your computer.

(over)

We know that keeping up with the latest security software, operating systems, and fraud scams can be challenging, so we've also collected information on how to protect yourself online. Visit our Security Center for tips on protecting your devices and personal information, and learn how Vanguard protects your personal and financial information.

Accounts that may be covered

Our reimbursement commitment covers accounts that you hold directly with Vanguard mutual funds and accounts with Vanguard Brokerage Services®, a division of Vanguard Marketing Corporation. If you participate in a retirement plan for which Vanguard provides recordkeeping and administrative services, your participant account is covered, too (unless the activity is performed by an employer or plan sponsor representative who is authorized to access your account, in which case your employer or the plan sponsor may provide reimbursement for the unauthorized activity).

Accounts that aren't covered

Our reimbursement commitment doesn't apply to unauthorized activity in annuities or 529 savings plan accounts.

Suspect fraud?

If you think your accounts could be compromised, we want to know.

We need to know immediately if you've been a victim of fraud. Please take the following steps:

Contact Vanguard immediately.

Contact us at **877-223-6977** or send an email to fraud@vanguard.com.

Conduct a full virus scan on all your computers and mobile devices.

You need to make sure you've removed any malicious code from your computers and devices before completing the next steps.

Change your credentials on all websites you log on to.

This includes your user name, password, and security questions. Also remember to change your email and social media accounts.

Alert the three major credit bureaus.

These companies monitor your credit activity and can block people from opening accounts using your information. Contact each credit bureau below:

Equifax

888-766-0008

Experian

888-397-3742

TransUnion

800-916-8800

Have you been a victim of identity theft?

If you've had your identity stolen within the last 12 months, and you're a Vanguard client, contact us immediately. You can send an email to fraud@vanguard.com and include your name, the circumstances of the criminal activity, and a phone number where we can reach you. Or call us at **877-223-6977** and provide the answers to the same questions. We'll begin investigating your concerns as soon as we receive your information, even if we don't get back to you right away.

Identity theft occurs when a criminal steals your personal information to access your accounts or open new accounts under your name. Some common ways unauthorized people can get your information include breaking into your house, intercepting your postal mail or email, sending phishing emails, and using the shared credentials of a family member.

Suspect fraud?

Call **877-223-6977**

Monday through Friday

8 a.m. to 7 p.m., Eastern time.

(over)

For more information on identity theft, visit the Federal Trade Commission (FTC) website. You'll get more information about this crime, see some helpful tips about how to protect yourself, and read about the latest scams.

[Visit the FTC's website](#)

Do you suspect phishing?

If you received an email claiming to be from Vanguard requesting your private information, please forward it to phish@vanguard.com immediately and let us know if you clicked any of the links in the message and/or entered your personal information on a website.