Keep your account information safe

As a Vanguard client, you can rely on us to make protecting your account information a priority. That's why we've implemented strict security policies and procedures that protect your assets and personal information.

You also play a part in keeping your personal information secure. Anyone with bank, credit card, and other financial accounts shares responsibility for safeguarding account information.

Measures that Vanguard takes to protect your account and personal information include the following:

- Instituting strong controls such as enhanced authentication and verification, transaction confirmations, notifications of certain account changes, and online timeout features.
- Restricting access to buildings, systems, and facilities only to authorized individuals.
- Limiting access to client information to those employees who need it to perform their jobs.
- Providing frequent training for employees on preventing fraud and protecting sensitive information.

This brochure examines signs of identity theft, how you can prevent it, and what to do if you suspect it's happened to you.

How to spot identity theft

Identity theft occurs when an impostor obtains key pieces of personal identifying information such as a Social Security number, name, address, date of birth, or driver's license number, and uses it for personal gain.

Signs that you might be a victim of identity theft include:

- Discovering accounts you didn't open or transactions on your accounts that you can't explain.
- Receiving confirmation of unauthorized address, phone number, or beneficiary changes on your accounts.
- Receiving confirmation of unauthorized online access to your accounts.
- Finding fraudulent or inaccurate information on your credit report.
- Failing to receive account statements, monetary or clerical confirmations, credit card bills, or other mail expected from your financial institutions.
- Receiving credit cards you didn't apply for.
- Unexpectedly being denied credit or being offered less favorable credit terms, like a high interest rate.
- Receiving calls or letters from debt collectors or businesses about merchandise or services you didn't purchase.

How you can safeguard your account and personal information

- Review statements and confirmations as soon as you receive them and notify your financial institutions immediately of any discrepancies.
- Shred financial documents and papers with personal information before you discard them.
- Protect your Social Security number and passwords.
- Don't allow anyone else, even a family member, to access your account online without having written documentation on file at your financial institution.
- If you don't access your accounts online, block them. That way, no one else can access them either.
- Sign up for security codes that prevent others from accessing your accounts without your knowledge.
- Don't provide personal information by phone, through the mail, or over the internet unless you know who you're dealing with.
- Never click links in unsolicited emails.

How to protect your online credentials

- Use strong passwords that include numbers, uppercase and lowercase letters, and special characters. Longer passwords are more secure.
- Don't use something easy to guess—like your birth date, your child's name, your pet's name, or "password"—as your password.
- Memorize your passwords and never write them down.
- Change your passwords often.
- Never give out a password over the phone or send it via email.
- Never share your user IDs and passwords with anyone.

How to secure your computer

- Use firewalls, antispyware, and antivirus software, and keep them up to date.
- Scan your computers for spyware often, ideally every day.
- Properly dispose of sensitive information. To ensure that an attacker can't obtain sensitive files, erase them from your computer.

How to respond to identity theft

If you're the victim of identity theft, immediately notify Vanguard and the other financial institutions where you hold accounts. Then place a fraud alert on your credit report.

A fraud alert informs companies to contact you before opening new credit accounts or issuing loans. To initiate a fraud alert, contact any one of the three major consumer reporting agencies shown below.

Tell the agency that you want an initial 90-day fraud alert, additional information on security freezes, and a copy of your credit report.

Calling one of the three agencies should be sufficient. The company that you call is required to contact the other two agencies.

You might want to consider these additional measures for responding to identity theft:

- Place a security freeze on your credit file at all three credit bureaus. This way, an identity thief can't open a new account because the potential creditor or seller of services won't be able to check the credit file.
- Review your credit report. A free annual credit report is available from each of the three consumer reporting agencies at annualcreditreport.com. Obtain new credit reports every three months for the next year as an added precaution, and review information about identity theft on the Federal Trade Commission website: ftc.gov/idtheft.
- Close compromised accounts. Contact financial institutions where you have investment, loan, or credit card accounts to inform them that your accounts may have been compromised. Close any accounts that have been tampered with or established fraudulently.

We recommend you call the security or fraud department of each company where an account was opened or changed without your consent. Ask for verification that the disputed account has been closed and the fraudulent debts discharged. Then carefully examine account statements and transaction confirmations to make sure they don't contain any activity that you didn't authorize.

Finally, keep copies of documents of your conversations about the theft, file a police report for creditors who may want proof of the crime, and report the theft to the FTC.

For more information, visit our Security Center at vanguard.com/securitycenter.

Consumer reporting agencies

- Equifax: **800-525-6285** or **equifax.com**
- Experian: **888-EXPERIAN** (**397-3742**) or **experian.com**
- TransUnion: **800-680-7289** or **transunion.com**

FRDBRO 012016