Identity theft is the use, or attempted use, of an account or identifying information without the owner's permission. Normally, identify theft involves stealing an individual's personal information and using it illegally for financial gain or other fraudulent purposes.

What if my personal information has been stolen and is being used?

Report it immediately, both by phone and in writing. Keep complete, accurate records of all contacts, including a log of phone calls and copies of all correspondence.

- Notify affected businesses such as banks, stores and other credit issuers.
- Alert the three major credit bureaus:
  - Equifax: equifax.com, 800-685-1111
  - TransUnion: transunion.com, 800-916-8800
  - Experian: experian.com, 800-397-3742
- File a report with your local police and request a copy.
- Contact the Federal Trade Commission, consumer.gov/idtheft, 877-ID-THEFT (438-4338) for further details about what to do.

You have more weapons against identity theft than you may think. Being aware of the threat and exercising common sense are two of the most important. Recognize that your personal information is valuable to thieves, and make safeguarding it part of your normal routine.

What is Raymond James doing to protect my personal information?

We devote extensive technological and human resources to securing the information you entrust to us. At our international headquarters in St. Petersburg, Florida:

- Physical security measures include on-site security officers, 24/7 video surveillance, employee identification badges, required visitor check-in and restricted access to critical areas;
- Technological safeguards include the latest firewalls, anti-virus programs and intrusion detection tools, along with 24/7 monitoring of our data systems for signs of unauthorized activity;
- Employee training requirements include comprehensive orientation in privacy and security policies, as well as ongoing security training for both our employees and our affiliated financial advisors;
- Business continuity planning ensures that all data remains secure in the event of business disruption due to a natural disaster or other emergency; and
- Industry-wide coordination enables us to collaborate with companies nationwide to share data security strategies and information.

By taking steps to protect yourself from identity theft, you can join us in helping to ensure that your personal information remains private and secure.

RAYMOND JAMES®

Individual solutions from independent advisors

International Headquarters:
The Raymond James Financial Center
880 Carillon Parkway | St. Petersburg, FL 33716
727-567-1000 | Toll-Free: 800-248-8863
raymondjames.com

SAFEGUARDING YOUR IDENTITY

Your Personal and Financial Information is Precious: Protect It by Being Savvy About Identity Theft

RAYMOND JAMES®

Am I at risk for identity theft?

Almost anyone can be a target. About 9 million U.S. adults, or 4% of the population, will be victims of identity fraud this year.

How does it work?

Identity thieves traffic in personal information of many kinds, including:

- Your name, address, phone number and date of birth,
- Bank account, Social Security, PIN and credit card numbers, and
- Other personal information, such as IDs and passwords, which can be used to access your protected bank accounts, online shopping accounts, credit card accounts and others.

Tactics range from simply snatching your wallet or purse to searching through your trash or watching you enter numbers at an ATM or checkout counter. Another strategy is contacting you by phone or e-mail, misrepresenting who is calling, and prompting you to give out private information.

More sophisticated and often large-scale methods involve hacking into computer systems; sending out spam that requests your personal information for some non-existent reason; and creating phony websites that are replicas of legitimate sites in order to get users to enter passwords, account numbers and other valuable personal information.

Once thieves have obtained this information, they may use it to:

- Make purchases using stolen credit card numbers. They may also change the credit card billing address so you won't receive statements that would show the fraudulent purchases;
- Create new credit lines for loans, credit card accounts or phone service, and then not pay the bills or open new bank accounts and write bad checks on them;
- File bankruptcy in your name to evade creditors or prevent eviction; or
- Obtain false credentials, such as a driver's license or ID card, and create a new identity to avoid being prosecuted for crimes.

How can I safeguard my personal information?

Take simple steps to help reduce your risk of identity theft.

- Keep personal information safely hidden in your home. Don't carry your Social Security card with you, and carry only those credit cards you need. Destroy old or expired cards.
- Secure your purse or wallet at work and elsewhere.
- Remember not to give out account numbers, passwords or other private information in response to e-mail, phone or in-person requests, or enter them on websites you don't know to be legitimate and secure.
- Eliminate as many paper statements, bills and checks as possible, using electronic transactions – such as online banking – instead. Close any inactive accounts.
- Avoid using obvious or common passwords, such as children's names or birthdates, on your accounts.
- Review all your accounts, as well as your credit report, regularly. Report any suspicious activity to the account issuer.[1]
- Check to make sure no one is lingering nearby before you give personal information over the phone or in person, or enter it into an ATM or other device.
- Shred documents before discarding and use only a secure mailbox for mail.

Be aware of the potential for computer-related identity theft.

- Update your computer's virus protection, firewall, browser security features and other privacy software tools regularly.
- Use only secure sites that have "https" in the URL and/or a padlock icon in the security status bar of your browser.
- Resist opening files or links sent from unknown sources. Instead, type the URL of the site you want directly into the address line rather than clicking a link.
- Encrypt personal information when necessary.
- Avoid storing personal information on a laptop computer unless absolutely necessary.
- Run a "wipe" utility to erase all information before disposing of any computer.

[1] You can obtain one free credit report per year at annualcreditreport.com or by calling 877-322-8228.

How will I know if I've been a victim of identity theft?

Often, the first clue is unusual activity on a credit card or bank account; receipt of a bill for an account you never opened; or failure to receive bills or statements for active accounts. The latter may indicate that a false change of address has been filed to prevent you from receiving statements and spotting unauthorized activity. Another "red flag" is unwarranted collection notices or calls.

If you are denied credit when you know you qualify, someone may have compromised your credit rating by using your account information. If your driver's license is being fraudulently used, it may be revoked or suspended for violations you didn't commit.