Your personal and financial information is precious. Protect it by being savvy about identity theft.
EVERYONE IS AT RISK FOR IDENTITY THEFT.

It’s an unfortunate statistic, but the Federal Trade Commission says about 9 million people are victims of identity theft each year. For some victims, problems are resolved quickly. But for others, it may cost hundreds of dollars and countless hours to repair damage done to their good names and credit records.

HOW IDENTITY THEFT WORKS

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

• Other personal information, such as IDs and passwords

Identity thieves use many methods for stealing information, including:

• Simple theft – This involves stealing wallets and purses; mail, including bank and credit card statements; pre-approved credit offers; and new checks or tax information.

• Over-the-shoulder spying – Thieves watch people enter numbers at ATMs or checkout counters.
• Dumpster diving – This includes rummaging through trash for bills or other paper containing personal information.

• Skimming – Credit/debit card numbers are stolen using a special storage device when processing a victim’s card.

• Phishing – A thief pretends to be a financial institution or company by calling or sending spam or pop-up messages to get someone to reveal personal information.

• Changing address – A thief will divert a victim’s billing statements to another location by completing a change of address form.

• Pretexting – Thieves use false pretenses to obtain personal information from financial institutions, telephone companies and other sources.

Once thieves obtain personal information, they may use it to:

• Make purchases using stolen credit card numbers – they may also change the credit card billing addresses so victims won’t receive statements showing fraudulent purchases

• Create new credit lines for loans, credit card accounts or phone service

• Open new bank accounts and write bad checks on them

• File bankruptcy in a victim’s name to evade creditors or prevent eviction

• Obtain false credentials, such as a driver’s license or ID card, and create a new identity to avoid being prosecuted for crimes

**TAKE STEPS TO SAFEGUARD PERSONAL INFORMATION**

Nothing guarantees you won’t be a victim. But you can take steps to lower your risk of identity theft.

• Shred financial documents and paperwork with personal information before you discard them – micro shredders work best

• Secure your purse or wallet at work and elsewhere

• Make sure no one is lingering nearby when giving personal information over the phone or in person, or entering it into an ATM or other device

• Protect your Social Security number by not carrying your card in your wallet or writing your Social Security number on a check – if possible ask to use another identifier

• Don’t give personal information on the phone, through the mail or over the Internet unless you have initiated the contact and know who you are dealing with
Use firewalls and up-to-date anti-spyware and anti-virus software on your home computer.

- Use only secure sites that have “https” in the URL and/or a padlock icon in your browser’s security status bar
- Never click on links sent in unsolicited emails
- Run a “wipe” utility to erase all information before disposing of any computer
- Avoid storing personal information on a laptop computer unless absolutely necessary
- Don't use obvious passwords like birth dates, mother's maiden name or the last four digits of your Social Security number
- Keep your personal information in a secure place at home, especially if you have roommates, employ outside help or have work done in your house
- Eliminate as many paper statements, bills and checks as possible, and use electronic transactions such as online banking – close inactive accounts.
- Review all your accounts, as well as your credit report, regularly. Report any suspicious activity to the account issuer
- Encrypt personal information when necessary

1 You can obtain one free credit report per year at annualcreditreport.com or by calling 877-322-8228.
HOW TO KNOW IF YOU’RE A VICTIM
The importance of reviewing account information cannot be stressed enough. Often the first clue is unusual activity on a credit card or bank account. Other signs include:

• Mail or bills that do not arrive as expected – this may indicate a false change of address has been filed to prevent you from receiving statements and spotting unauthorized activity
• Unexpected credit cards or account statements
• Denials of credit for no apparent reason
• Calls or letters about purchases you did not make
• Receipt of a bill or an account you never opened
• Your driver’s license is revoked or suspended for violations you didn’t commit

WHEN PERSONAL INFORMATION HAS BEEN STOLEN
It’s important to take action as soon as you suspect a problem to reduce further harm.

• Report it immediately, 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, 888-397-3742
• 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.

AT RAYMOND JAMES, WE WORK HARD TO PROTECT YOUR PERSONAL INFORMATION.

We devote extensive technological and human resources to secure your personal information 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.

• 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 with us to help ensure your personal information remains private and secure. For additional information, visit http://www.ftc.gov/idtheft.*