

# **SAFEGUARDING YOUR IDENTITY**

---

**Take Charge to Prevent Identity Theft**

**The Cavalena Group at Raymond James Financial Services**

# **A Message from Raymond James**

**At Raymond James, our business is people  
and their financial well-being.**

The growing crime of identity theft threatens people's sense of security and peace of mind. That's why we're working to educate consumers about protecting their valuable personal and financial information against fraudulent use. It's simply part of our commitment to helping individuals and families build a financially secure and independent future.

# Working to Keep Your Confidence

- **Ensuring your privacy is a top priority at Raymond James.** We devote extensive technological and human resources to protecting the information you entrust to us.
  - Physical security
  - Technological security
  - Employee training
  - Business continuity
  - Industry-wide coordination

# Working to Keep Your Confidence: **Physical Security**

- At our international headquarters in St. Petersburg, Florida:
  - Security guards on site 24/7
  - Security desk staffed during business hours for visitor check-in
  - Employee identification badges required
  - Video surveillance of high-traffic areas, restricted-access areas and building exteriors

# Working to Keep Your Confidence: **Technological Security**

- 24/7 monitoring of technological systems for signs of tampering or unauthorized activity
- The latest firewall and anti-virus tools, plus specialized programs to prevent and detect intrusion
- Strict controls to limit employee access to computer systems

# Working to Keep Your Confidence: **Employee Training**

- Newly hired associates receive comprehensive information about our privacy policies and procedures as well as initial training in security awareness
- All employees must regularly attend additional training in ethics and security
- Regulatory compliance specialists ensure that we meet the requirements of federal legislation regarding customers' privacy
- Our affiliated financial advisors throughout the United States receive training at national conferences; past sessions include an FBI presentation on information security

# Working to Keep Your Confidence: **Business Continuity**

- Our professional Business Continuity team focuses on ensuring uninterrupted critical operations and preserving data security, even during emergency situations
- The team oversees management of our remote operations center and emergency functions such as data retention, backup procedures and off-site information storage

# Working to Keep Your Confidence: **Industry-wide Coordination**

- Raymond James executives play active roles in industry-wide organizations devoted to sharing information about physical and cyber security.
  - Thomas A. James, chairman and Chief Operating Officer, is chairman of the Financial Services Roundtable, an association representing 100 of the nation's largest integrated financial services companies.

# What You Can Do

- Raymond James devotes extensive technological and human resources to safeguarding the information you entrust to us. But we want you and your family to be able to protect yourselves, too.
- **The more you know about identity theft, the better you can protect yourself.**

# Understanding Identity Theft

## I Definition

## I Statistics

## I Action

- Know how ID theft works.
- Take steps toward prevention.
- Be alert.
- Report it.

# Definition

- ***Identity theft*** is the use, or attempted use, of an account or identifying information without the owner's permission.
- It normally involves stealing an individual's personal information (identity fraud) and using it illegally for financial gain or other, fraudulent purposes.

# Statistics

- About 9 million U.S. adults will be victims of identity fraud this year.
- The average fraud amount per case is almost \$6,400.
- Victims spend an average of 40 hours resolving ID fraud issues.

*Source: Better Business Bureau 1/06*

# Statistics

## **In a recent study:**

- Almost half of the victims detected the identity fraud themselves.
- 47% of victims identified the source of the theft.
- 36% of victims identified the person who misused their information. Almost half were individuals the victim knew.

*Source: Better Business Bureau 1/06*

# Statistics

## **In a recent study (cont.):**

- Average out-of-pocket cost for ID theft victims was \$422, but 68% of victims had no out-of-pocket costs at all.
- Adults 65+ have the lowest rate of ID fraud; adults 25-34 the highest.
- Internet use accounted for less than 10% of ID fraud cases. In fact, the study concluded that Internet use can lead to lower damages and faster detection.

*Source: Better Business Bureau 1/06*

# Action

- Know how ID theft works.
- Take steps toward prevention.
- Be alert.
- Report it.

# **Action: Know How ID Theft Works**

## **■ What do identity thieves want?**

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

# Action: Know How ID Theft Works

## How do the thieves get your information?

### I Low-tech strategies include:

- *Stealing* credit cards, wallets or checkbooks
- *Watching or listening* when you give information by phone or in person, or enter numbers at ATMs, checkout counters, and elsewhere (called “shoulder surfing”)
- *Going through your trash* to obtain personal identifying information from discarded documents (called “dumpster diving”)

# Action: Know How ID Theft Works

## I Low-tech strategies (cont.):

- *Phoning you and asking you to provide personal data* in order to obtain some benefit or avoid some threat
- *Filing change of address forms* to divert your mail – bank and credit card statements, checks, etc.
- *Masquerading* as an employer or landlord to fraudulently obtain your credit report

# Action: Know How ID Theft Works

## I High-tech strategies include:

- *Hacking into computer systems* and extracting data
- *Using electronic “skimmers”* to capture data from ATMs and other devices
- *Distributing mass e-mails* directing recipients to provide identifying data in order to obtain some benefit or avoid some threat
- *Creating replicas of legitimate Web sites* or pages to fool the user into submitting personal, financial or password data (called “phishing”)

# Action: Know How ID Theft Works

- High-tech strategies (cont.):
  - *Placing codes on legitimate Web sites* to divert data to phony look-alike sites
  - *Planting software on home computers* to monitor the user's activity, including keystrokes for entry of passwords often through viruses and peer-to-peer networks
    - Or to take control of your computers resources to propagate spam and phishing attacks against others

**ID thieves are constantly developing new technological strategies.**

# **Action: Know How ID Theft Works**

## **I How do ID thieves use the information?**

- Make purchases using stolen credit card numbers, or open new bank accounts and write bad checks
- Create new credit lines for loans, credit cards or phone service, and then not pay the bills
- Drain your bank account through counterfeit checks, stolen credit/debit cards or fraudulent electronic transfers
- File bankruptcy in your name to evade creditors or prevent eviction
- Assume a new identity – yours – to avoid being prosecuted for crimes

# **Action: Take Steps Toward Prevention**

**Simple steps can help you avoid becoming a victim of identity theft and fraud.**

- General precautions
- Account management precautions
- Computer precautions

# Action: Take Steps Toward Prevention

## General precautions

- **Do** keep all personal information, including passwords and account numbers, securely hidden in your home.
- **Do** secure your purse or wallet at work and elsewhere.
- **Do** 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.

# Action: Take Steps Toward Prevention

## General precautions (cont.)

- **Do** use only secure mailboxes for incoming and outgoing mail.
- **Do** shred personal documents before discarding.
- **Do** ask about security procedures of companies where you do business.

# Action: Take Steps Toward Prevention

## General precautions (cont.)

- **Don't** carry your Social Security card with you, and carry only those credit cards you need.
- **Don't** give out your Social Security number, account numbers, passwords or any other private information in response to e-mail, phone or in-person requests you don't know to be valid.
- **Don't** enter personal information on Web sites you don't know to be both legitimate and secure.

# Action: Take Steps Toward Prevention

## Account management precautions

- **Do** use electronic transactions – such as online banking – instead of paper statements, bills and checks.
- **Do** close any inactive accounts and destroy old or expired credit cards.
- **Don't** write the full account number on checks when paying bills; just use the last four digits.

# **Action: Take Steps Toward Prevention**

## **Account management precautions (cont.)**

- I Do** check credit card statements against receipts.
- I Do** routinely monitor all your accounts and report any suspicious activity to the account issuer.
- I Do** review your credit report regularly. By law, you can obtain one free credit report per year by calling 877-322-8228 or at <http://www.annualcreditreport.com>.

# Action: Take Steps Toward Prevention

## Computer precautions

- ! **Do** keep your computer's virus protection, firewall, browser security features and other privacy software tools up to date.
- ! **Don't** open files or links from unknown sources.
- ! **Do** type the URL of the site you want directly into the address line, rather than clicking on a link.
- ! **Don't** use obvious online passwords like birthdates or names. Change passwords frequently.

# Action: Take Steps Toward Prevention

## Computer precautions (cont.)

- **Don't** store personal information on a laptop computer unless absolutely necessary.
- **Do** use only secure banking, shopping or other business Web sites that have "https" and/or a padlock icon in the URL or the status bar across the bottom of your browser, signifying that all transactions are secured.
- **Don't** dispose of a computer before running a "wipe" utility, which is the only way to completely erase all information.

# **Action: Be Alert**

**Watch for signs that your personal information is being misused.**

## **I Unusual financial activity**

- Charges or withdrawals you didn't authorize on credit card or bank accounts
- Receipt of a bill for an account you didn't open
- Failure to receive bills or statements for active accounts

# Action: Be Alert

## ■ Unwarranted financial problems

### Examples:

- **Being contacted by collection agencies or businesses** about bills or other transactions you didn't create
- **Having your credit affected** because someone may have compromised your credit rating by using your account information

# Action: Be Alert

## I Other legal or financial surprises

### Examples:

- **Receiving credit cards** you didn't apply for.
- **Bouncing checks** because of unauthorized withdrawals from your account.
- **Having your driver's license revoked.** If your license is being fraudulently used, it may be revoked for violations you didn't commit.

# **Action: Report It**

**Many public and private agencies are working together to fight identity theft.**

**By notifying them that you have been a victim, you help them track down the offenders.**

# Action: Report It

## What to do if you are a victim of ID theft

- **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.
- **File a report with your local police** and request a copy.

# Action: Report It

## What to do (cont.)

- ! Alert the three major credit bureaus:
  - ! Equifax: [www.equifax.com](http://www.equifax.com), 800-525-6285
  - ! Experian: [www.experian.com](http://www.experian.com), 888-397-3742
  - ! TransUnion: [www.tuc.com](http://www.tuc.com), 800-680-7289
  
- ! Contact the Federal Trade Commission,  
<http://www.consumer.gov/idtheft>, 877-438-4338

# Action: Report It

## What to do (cont.)

- **If your Social Security card has been stolen**, contact the Social Security Administration, [www.ssa.gov](http://www.ssa.gov), for a replacement card.
- **If the theft involves your mail**, contact the nearest Postal Inspection Service office. Locate it at <http://www.usps.com/ncsc/locators/find-is.html>
- **If your driver's license has been stolen**, contact the issuing office to cancel it and obtain a replacement.

# **Now: Take Charge**

**You're better armed against identity theft than you think.**

- Being aware of the threat and exercising common sense are two of your most valuable weapons.
- Recognize that your personal information is valuable to thieves, and make safeguarding it part of your normal routine.
- Take advantage of the many resources available to educate yourself and your family about identity theft.

## For More Information

- The Federal Trade Commission's identity theft Web site ([http://www.consumer.gov/idtheft/con\\_steps.htm](http://www.consumer.gov/idtheft/con_steps.htm)) is a comprehensive online resource. You can also call the FTC at 877-438-4338 and request printed materials about identity theft.
- The Better Business Bureau (<http://www.bbbonline.org/IDTheft>) site contains valuable reports and articles about new ID theft tactics and measures to protect you and your family.
- [www.lookstoogoodtobetrue.com](http://www.lookstoogoodtobetrue.com) is a site sponsored jointly by the federal government and private industry. It includes consumer alerts, new scams under way, reports of actual identity theft cases, and other useful information.
- [www.fightidentitytheft.com](http://www.fightidentitytheft.com) is a privately-developed site that includes the latest news about identity theft and fraud, preventive strategies, online discussion forums and a great deal of practical information for consumers.

## For More Information (cont.)

- [www.annualcreditreport.com](http://www.annualcreditreport.com) is the central site where you can request your free credit file disclosure, commonly called a “credit report,” once every 12 months from each of the nationwide consumer credit reporting companies. You are entitled by law to these free reports.
- [www.onguardonline.gov](http://www.onguardonline.gov) provides practical tips from the federal government and the technology industry to help consumers guard against Internet fraud, secure their computers and protect personal information.
- The Internet Crime Complaint Center ([www.IC3.gov](http://www.IC3.gov)) is specifically devoted to “cyber crime,” including identity crimes carried out via the Internet. Sponsored by the FBI and the National White Collar Crime Center, IC3 provides valuable alerts regarding the newest types of cyber crimes.

# **A Final Thought**

Identity thieves are looking  
for ways to steal your  
valuable personal information.

Your best defense is  
taking steps to protect it.

This presentation is a service of:

The Cavalena Group @



1006 N. Wooster Ave | Dover, Ohio 44622  
330.343.2212 | 800.837.7276  
[www.raymondjamesohio.com](http://www.raymondjamesohio.com)