

# **IDENTITY THEFT PROTECTION:**

## **DON'T BE A VICTIM**

**Presented by:**  
**James J. Holtzman, CFP®**  
**Wealth Advisor and Shareholder**  
**Legend Financial Advisors, Inc.®**

## **JAMES J. HOLTZMAN, CFP®**

**James J. Holtzman, CFP®, is a Wealth Advisor and Shareholder with Legend Financial Advisors, Inc.® and Emerging Wealth Investment Management, Inc.®**

**Jim has been selected eight consecutive times by *Medical Economics* as one of “The 150 Best Financial Advisors for Doctors in America.”**

**Mr. Holtzman has been selected five times by *Dental Products Report* as one of “The Best Financial Advisors for Dentists in America”.**



**Jim has also been previously selected three times by *Pittsburgh Magazine* as one of the Pittsburgh area’s FIVE STAR Wealth Managers, a list that represents the most elite financial advisors in Pittsburgh.**

**With over 20 years of experience, Jim assists all types of clients with their financial planning and investment needs. Jim’s extensive skill set includes providing financial advice to retirement-focused clients, medical and dental practices, and businesses.**

**Jim serves as the firm’s Income Tax and Education Funding and Planning Specialist.**

**Jim’s previous professional experience includes employment with various CPA and Financial Advisory organizations where he provided tax, accounting, auditing and financial consulting services to individuals and businesses. Jim has also provided financial advice to various Fortune 500 and public company executives.**

**Jim’s areas of concentration include income tax planning, estate planning, stock option exercise planning, insurance, retirement planning and Section 529 Plans.**

**Mr. Holtzman was selected by *Pittsburgh Business Times* as one of the 2013 Fast Tracker's, which honors leaders in the Pittsburgh area's business community who've had a significant impact on the growth of their organization.**

# **TYPES OF IDENTITY (ID) THEFT**

- 1. Financial**
- 2. Insurance**
- 3. Medical**
- 4. Criminal**
- 5. Driver's License**
- 6. Social Security**
- 7. Tax**
- 8. Synthetic**
- 9. Change of Address**
- 10. Employment**

# **SYNTHETIC ID THEFT**

**1. Creates New Identity**

**2. Example:**

- a. Social Security Number From One Person**
- b. Fake Address**
- c. Phone Number From Another Person**

# **SOCIAL SECURITY ID THEFT**

- 1. Obtain New Social Security Cards**
- 2. Steal Social Security Benefits You Earned**
- 3. Create Passports, Etc.**

# **SOCIAL SECURITY ID THEFT**

- 1. Review Social Security Earnings Statement For Incorrect Information**
- 2. Social Security Administration Does Not Call Individuals**

# **CRIMINAL ID THEFT**

- 1. Thieves Commit Crimes Under Your Name**
- 2. Must Convince Courts That You Are The Victim**

# **DRIVER'S LICENSE ID THEFT**

- 1. Traffic Violations In Your Name**
- 2. Suspended License**



# **EMPLOYMENT ID THEFT**

- 1. Someone Works Under Your Name**
- 2. Incorrect Tax Reporting**
- 3. Claiming Of Unemployment Benefits**
- 4. Review Social Security Statement**

# **FINANCIAL ID THEFT**

- 1. Drain Your Bank Accounts**
- 2. Apply For Loans**
- 3. Open Credit Cards**

# **TAX RETURN ID THEFT**

- 1. Filing False Tax Returns To Collect Refunds**
- 2. Only Need Name and Social Security Number**
- 3. IRS Reconciles W-2 and 1099 Information After Refunds Are Issued**

# **WAYS TO IDENTIFY MEDICAL IDENTITY THEFT**

- 1. Reaching Benefit Limit**
- 2. Review Explanation Of Benefits Statement**
- 3. Request Health Insurance Benefits Statement**
- 4. Request Medical Records**
- 5. Review Credit Report**
- 6. Request “Accounting Of Disclosures” From Health Insurance And Healthcare Providers.**
  - a. Shows Who Receives Your Medical Records**

# **MAIN MEDICAL IDENTITY THEFTS**

- 1. Bill Health Insurance For Fake Claims**
- 2. Prescription Drugs**
- 3. Free Treatment**
- 4. Employee Error**
- 5. Electronic Medical Records**

# **MEDICAL IDENTITY THEFT CONSEQUENCES**

- 1. Unpaid Bills**
- 2. Max Out Coverage Limits**
- 3. Incorrect Medical Advice**
- 4. Increased Health Insurance Premiums**

# **CHILD IDENTITY THEFT**

- 1. Parents Aren't Paying Attention**
- 2. Impact Employment And Credit History**
- 3. Social Security Numbers - Sold To Human Traffickers/  
Thieves**
- 4. June, 2011 – Randomized Social Security Numbers**
- 5. Before June 2011, Social Security Numbers  
Based On When And Where Child Was Born**

# **CHILD IDENTITY THEFT (Continued)**

- 6. Health Care Providers/Schools Are Targets**
- 7. Parent Must Prove They Are The Parent**
- 8. Credit Reporting Services: Add Child**



# **HOW TO IDENTIFY CHILD IDENTITY THEFT**

- 1. Child Receives Pre-Approved Credit Cards**
- 2. Account Opening Denial**
- 3. Credit Report Exists**
- 4. Receive Bills For Products Not Used**
- 5. IRS Notice**

# **ELDER IDENTITY THEFT**

- 1. Usually Have Better Credit, More Home Equity**
- 2. Caregivers And Family Are Common Thieves**
- 3. Not Actively Using Credit Report**
- 4. Too Embarrassed To Report**
- 5. Hack Social Security Administration Death Master File**
- 6. Long-Term Care Facility Employee Background Checks**
- 7. Credit Freeze**

# **ELDER IDENTITY THEFT (Continued)**

## **Most Common Forms Of Identity Theft And Financial Scams**

- 1. Investment Fraud**
- 2. Mortgage Fraud**
- 3. Phone Solicitations**
- 4. Check Cashing Fraud**
- 5. Credit Card Fraud**
- 6. Forging Signatures**
- 7. Tax And Government Benefits Theft**
- 8. Medical Identity Theft**
- 9. Long-Term Care Identity Theft**
- 10. Caregiver Theft**

# **IDENTITY THEFT METHODS**

- 1. Dumpster Diving/Shoulder Surfing**
- 2. Vishing: Calls Requesting Personal Data**
- 3. Phishing: Emails Requesting Personal Data**
- 4. Smishing: Texts Requesting Personal Data**
- 5. Stolen Wallet/Mail Theft**
- 6. Change Of Address**

# **IDENTITY THEFT METHODS (continued)**

- 9. ATM Skimmer - Collect PIN**
- 10. Data Breach – Doctor Office, Department Store**
- 11. Fraudulent Websites**
- 12. File Sharing – Music, Pictures**
- 13. Overlay – Fake Keypad Over ATM Keypad**

# **HOW TO RECOGNIZE IDENTITY THEFT**

- 1. Receiving Collection Calls**
- 2. Unknown Accounts On Credit Report**
- 3. Denied Credit**
- 4. Credit Report Inquiries From Unknown Companies**
- 5. Stop Receiving Mail From Credit Cards**
- 6. Credit Or Debit Cards Are Missing**
- 7. Receive Bills For Accounts That Aren't Yours**
- 8. Bank Statement Transactions**

# **HOW TO RECOGNIZE IDENTITY THEFT (Continued)**

- 9. Bank Calls You About Irregular Activity**
- 10. Medical Insurance Explanation Of Benefit Statement**
- 11. Medicare Insurance Benefit Maximum**
- 12. Tax Return Efiling Rejection**
- 13. You Are Arrested For A Crime That You Did Not Commit**

# **STRATEGIES TO PREVENT IDENTITY THEFT**

- 1. Never Give Out Social Security Number**
- 2. Don't Write Passwords Down**
- 3. ATM Machine Precautions**
- 4. Avoid Online Prizes**
- 5. Garbage Surfing**
- 6. Keep Credit Card In Sight**



# **STRATEGIES TO PREVENT IDENTITY THEFT (Continued)**

- 7. Shred Everything**
- 8. Two-Factor Authentication**
- 9. Safe Disposal Of Computer, External Hard Drive, Etc.,**
- 10. Don't Leave Paid Bills In The Mailbox**
- 11. Don't Write Social Security Number Or Drivers License Number On Checks**
- 12. Don't Carry Social Security Card In Wallet**

# **STRATEGIES TO PREVENT IDENTITY THEFT (Continued)**

- 13. Avoid Social Security Number In Usernames Or Passwords**
- 14. Store Personal Information In A Safe Place**
- 15. Don't Respond To Unsolicited Requests For Information Online, Phone, Etc.**
- 16. Virus Detection Software**
- 17. Firewalls On Your Computer**
- 18. Do Not Carry Unused Credit Cards**
- 19. Operating System Is Up To Date**

# **STRATEGIES TO PREVENT IDENTITY THEFT (Continued)**

- 20. Credit Freeze**
- 21. IRS Does Not Contact By E-mail, Social Media, Texting, Or Telephone**
- 22. Purchase A Locking Mailbox**
- 23. Don't Carry Checkbook With You**
- 24. Use Encrypted E-mail**
- 25. Pick Up New Checks At The Bank**
- 26. Opt Out Of Prescreened Credit Offers**

# **STRATEGIES TO PREVENT IDENTITY THEFT (Continued)**

**27. Anti-Spyware Software**

**28. Safe Disposal Of Smart Phone Memory  
Card**

**29. Secure Home Wi-Fi Network**

**30. Don't Close Browser Before Logging Out  
Of Website**

# **SAFEGUARDING PERSONAL INFORMATION WHEN TRAVELING**

- 1. Backup Credit Card**
- 2. Separate Credit Cards**
- 3. Monitor Card Activity**
- 4. Write Contact Information For Credit Cards In A Safe Place**
- 5. Set Up A Separate Bank Account For Trip**
- 6. Inform Credit Cards Company And Bank About Traveling**
- 7. Limit Information In Wallet**

# **SAFEGUARDING YOUR PERSONAL INFORMATION WHEN YOU ARE TRAVELING (Continued)**

**8. Provide Someone You Trust With Financial Information**

**9. Change ATM/Debit Card To ATM Only. Requires PIN**

**10. Hold Mail At Personal Residence**

**11. Secured Wi-Fi Hotspots – Also On Cell Phone**

**12. Cell Phone - Use Secured Wi-Fi Hotspot**

**13. Do Not Post Vacation Places On Social Media Websites**

# **REPAIR IDENTITY THEFT**

- 1. Change Online Username And Passwords**
- 2. Fraud Alert**
- 3. Close Affected Bank Accounts**
- 4. Obtain Credit Report**
- 5. File Complaint With Federal Trade Commission (FTC)**
- 6. File Criminal Report With The Police**
- 7. Notify All Credit Reporting Agencies**

# **REPAIR IDENTITY THEFT**

## **(continued)**

- 9. Put Disputes In Writing**
- 10. Hire An Attorney**
- 11. File IRS Form 14039**
- 12. Contact The IRS Identity Protection Specialized Unit (800) 908-4490.**
- 13. Replace Lost Or Stolen Government Identification, such as Passports.**



# **IDENTITY THEFT REPORT (IDENTITY THEFT AFFIDAVIT)**

- 1. File Report With Federal Trade Commission (FTC)**
- 2. Removes Incorrect Information From Credit Report**
- 3. Stops The Debt From Being Sold To Collection Agency**
- 4. Extended Fraud Alert**
- 5. Identity Theft Report Consists Of The Following:**
  - 1. Identity Theft Affidavit**
  - 2. Police Report**

**<http://www.consumer.ftc.gov/articles/pdf-0094-identity-theft-affidavit.pdf>**

# **TOP 12 TAX FRAUDS ANNOUNCED BY THE IRS**

- 1. Tax Return Refunds**
- 2. Telephone Scams**
- 3. Phishing**
- 4. Free Money From Inflated Refunds**
- 5. Return Preparer Fraud**
- 6. Hiding Income Offshore**
- 7. Impersonating Charitable Organizations**

# **TOP 12 TAX FRAUDS ANNOUNCED BY THE IRS (continued)**

- 8. False Income, Expenses Or Exemptions**
- 9. Frivolous Arguments**
- 10. Claiming Zero Wages Or False Form 1099**
- 11. Abusive Tax Structures**
- 12. Misuse Of Trusts**

# **2017 TAX SEASON**

- 1. Security Summit**
  - A. The IRS**
  - B. Tax Preparation Software Firms**
  - C. Payroll Companies**
  - D. State Tax Administrators**
- 2. Software Companies Using Better Identity Validation**
- 3. States Working With Banks - Refunds Are Going Into Accounts That Match The Tax Return**
- 4. W-2 Verification Code For Professional Software**
- 5. Early Warning System On New Trends, Etc.**

# **SOFT CREDIT INQUIRY**

- 1. Does Not Affect Credit Score**
- 2. Recorded In Credit History But Not Visible To Lenders**

## **Examples:**

- a. Checking Your Own Credit**
- b. Pre-approval Credit Checks**
- c. Credit Check By Existing Credit Cards, Insurance Companies, Etc.**
- d. Pre-employment Screenings**

# **HARD CREDIT INQUIRY**

- 1. When You Give Lender Permission To Check Credit**
- 2. Approximately 5 Point Drop In Credit Score**
- 3. When Interest Rate Shopping, One 5 Point Drop**
- 4. Remain On Credit Report Up To 2 Years**

## **Examples:**

- a. Credit Card Application**
- b. Any Type Of Loan**
- c. Cell Phone Account Opening**

# **FRAUD ALERT**

- 1. Free Service**
- 2. Credit Reporting Agencies Offer Them**
- 3. Alerts Potential Lenders Identity Might Be Stolen**
- 4. Only Need To Call One Credit Reporting Agency**
- 5. Lenders Verify Identity - Not Required**
- 6. Initial Alert: 90 Days**

# **FRAUD ALERT (continued)**

- 7. Renew After 90 Days**
- 8. Obtain Free Credit Report – Each Agency**
- 9. Removed From Pre-approved Credit – 2 Years**
- 10. Alert Lenders/Creditor That Fraud Alert In Place**
- 11. Extended Fraud Alert: 7 Years**
  - a. Need To Provide Identity Theft Report**



# **CREDIT FREEZES**

- 1. Prevents Creditor Access To Credit Report**
- 2. Place With Each Credit Reporting Agencies**
- 3. Remains Until You Remove It**
- 4. \$3.00 - \$10.00 Per Credit Reporting Agency**
- 5. Small Fee To Unthaw Credit Report**

# **CREDIT FREEZES (Continued)**

**7. Will Be Provided PIN**

**8. Does Not Impact Credit Score**

**9. Provide The Following To Unthaw Credit:**

- ID Verification**
- Provide PIN**
- Identify Who Can Access Credit Report**

**10. Will Not Apply To Existing Credit**

# **IDENTITY THEFT SERVICES**

**Most Popular: Equifax, Experian, TransUnion, Lifelock**

## **Typical Services**

- 1. Identity Monitoring**
- 2. Fraud Alerts**
- 3. Resolution Services**
- 4. Stolen Wallet Assistance**
- 5. Insurance**
- 6. Mail List Removal**
- 7. Credit Monitoring**
- 8. Credit History Reports**
- 9. 24/7 Phone Support**
- 10. Daily Monitoring**
- 11. Social Security Number Monitoring**

# **DIFFERENCE BETWEEN CREDIT AND IDENTITY MONITORING**

- 1. Credit Monitoring: Monitors Credit Reports**
- 2. Identity Monitoring: Alerts You When Personal Information Is Used And Will Not Show Up On Credit Report**
  - a. Social Media**
  - b. Court Records**
  - c. Dark Web**
  - d. Utility Service Orders**

# **REGISTRATION SERVICES**

- 1. Tracks Credit/ Debit Card Information**
- 2. Report Lost Cards To Issuing Card Company**
- 3. Request Replacement Credit/Debit Cards**
- 4. Cost For This Service**
- 5. Issuing Card Company Might Not Accept Registration Service Request**

# ATM/DEBIT CARD LOSS

## IF YOU REPORT

## YOUR MAXIMUM LOSS

**Before any unauthorized charges**

**\$0**

**Within 2 business days after you learn about the loss or theft.**

**\$50**

**More than 2 business days after you learn about the loss or theft, but less than 60 calendar days after your statement is sent to you**

**\$500**

**More than 60 calendar days after your statement is sent to you.**

**All the money taken from your ATM/debit card account, and possibly more; for example, money in accounts linked to your debit account.**

# **CREDIT CARD LOSS**

- 1. Liability For Unauthorized Use: \$50.00**
- 2. No Liability If Loss Is Reported Before It Is Used**

# HOW TO REVIEW YOUR CREDIT REPORT

1. Review Name (Especially Middle Initial)
2. Address
3. Social Security Number
4. Employers
5. Accounts That Are Not Yours
6. Late Payment
7. Go To [www.annualcreditreport.com](http://www.annualcreditreport.com) Or Call 1-877-322-8228 For Free Credit Report



# **HOW TO HANDLE ERRORS ON CREDIT REPORTS**

- 1. Write Letters To All 3 Nationwide Credit Reporting Agencies**
- 2. Write Letter To Company That Has Incorrect Information**
- 3. Business Has 30 Days To Respond**
- 4. Credit Reporting Agency Must Do The Following**
  - a. Send Details Of Any Change**
  - b. Block Identity Theft Information From Your Credit Report**
  - c. Tell Business That Sent Incorrect Information About The Error**
  - d. Tell You If They Reject Your Claim**

# **HOW IDENTITY THEFT AFFECTS YOUR CREDIT SCORE**

- 1. Can Lose Hundreds Of Points From Credit Score**
- 2. Higher Balances On Credit Cards**
- 3. New Accounts**
- 4. Late Payments On New Accounts Opened**
- 5. Too Many Inquiries**
- 6. File Tax Returns – Unpaid Liability**
- 7. Obtain Bogus Checks**
- 8. Open A Fake Business In Your Name**

# **CREDIT REPORT CHANGES**

- 1. State Attorney Generals Settlement May 31, 2015**
- 2. Deadline: May 31, 2018**
- 3. Credit Reporting Agencies Obligations:**
  - a. Medical Debts Cannot Show Up On Credit Report Until After 180 Days After Is Reported**
  - b. Assign Experts To Investigate Identity Theft, Mixed Files And Fraud**
  - c. Cannot Pitch Services While Fixing Credit Report Mistake**

# **CREDIT REPORT CHANGES (CONTINUED)**

- 4. Provide Additional Free Credit Report To Prove The Dispute Has Been Fixed**
- 5. Share Data To Credit Issuers In A Dispute**
- 6. Notify The Other Credit Reporting Agencies Of Errors In A File**
- 7. Debt Collectors Must Provide Creditor's Information**

# **CREDIT SCORE UPDATE**

- 1. Begins July 1, 2017**
- 2. Credit Reporting Agencies Are Dropping Tax License and Civil Judgments Without Complete Data**
- 3. Complete Data Is The Following:**
  - a. Names**
  - b. Addresses**
  - c. Social Security Numbers Or Dates Of Birth**

# **ITEMS NO LONGER REPORTABLE TO CREDIT AGENCIES**

- 1. Any Debts Not Associated With A Contract Or Agreement By A Consumer**
  
- 2. Examples**
  - a. Traffic Tickets/Fines**
  - b. Parking Tickets/Fines**
  - c. Toll Road Fines**
  - d. Library Fees**

# **IS ID THEFT INSURANCE WORTH IT?**

- 1. Average Benefit Is Between \$10,000.00 And \$20,000.00**
- 2. No Out-Of-Pocket Costs Are Incurred 50.0% Of The Time**
- 3. Biggest Burden Is Time**
- 4. Fixing Credit - Average Time Spent Is 4 Hours**
  - a. But 10% Of Victims Spent More Than 55 Hours**
- 5. Resolution Services**
- 6. Does Policy Help With Medical, Criminal And Other Issues**
- 7. Does Policy Help With Hiring A Lawyer**
- 8. Banks May Provide This Insurance**
- 9. Homeowners/Renters Insurance Policy**

# **IS ID THEFT INSURANCE WORTH IT? (Continued)**

**10. Average Cost Is Between \$25.00 And \$60.00 Annually**

**11. Deductibles Can Range Form \$100.00 And \$150.00**

**12. What The Policy Can Cover**

**a. Credit Alerts**

**b. Credit Monitoring**

**c. Reimbursement For Costs To Repair Credit**

**d. Limited Lost Wages**

**13. What The Policy Does Not Cover**

**a. Reimburse Assets**

**b. Identity Theft If Caused By Family Member**



# **INTERNET**

- 1. HTTP: Hypertext Transfer Protocol – No Encrypted**
- 2. HTTPS: Hypertext Transfer Protocol Secure**

# **CREDIT CARD NUMBERS**

- 1. The First Digit – Card Issuer  
(Example 3 Is For American Express)**
- 2. The Next Five Digits - Bank That Issues Card**
- 3. Remaining Digits - Account Number And One Or More Check Digits**
- 4. Check Digit - Applied To Formula Verifying Credit Card**
- 5. Security Numbers Verify Identity When Card Is Not Present (Internet Or Phone Orders)**

# MISCELLANEOUS

- 1. Checking Account Opened In Your Name**
  - a. Chexsystems Report – Lists Checking Account Opened In Your Name**
    - i. Provides Information About Check Overdrafts, Unsettled Balances, Fraudulent Check Deposits**
- 2. Bankruptcy Filed In Your Name**
  - a. Contact U.S. Trustee In The U.S. Region Where Bankruptcy Was Filed**
- 3. Brokerage Account**
  - a. Contact SEC With A Complaint**
  - b. Contact Brokerage Firm**

# **IDENTITY THEFT AGAINST YOUR FINANCIAL ADVISOR**

**1. Scammer Hacks E-mail Account**

**2. E-mail Request Appear To Be From A Client**

**3. Advisor Should Contact You About Any  
Money Movement Request**

# **ACTIVE MILITARY DUTY**

- 1. If Deployed, Have An “Active Duty Alert”  
On Your Credit Report**
- 2. Last For 1 Year**

# **FEDERAL TRADE COMMISSION**

**[www.ftc.gov](http://www.ftc.gov)**

- 1. Has Sample Letters To Use For Disputes**
- 2. Annual Credit Report Request**
- 3. FTC Identity Theft Affidavit**
- 4. Contact Information For Credit Reporting Companies, Departments Of Federal Government**

# **INTERNET OF THINGS (IOT)**

- 1. Definition – Devices Connected To The Internet**
- 2. Examples: Refrigerator, Thermostats, Home Security Devices, Medical Devices**
- 3. Fitbit Might Have Date Of Birth, Name And Address**
- 4. Keep IOT On Separate Networks**
- 5. Update Security Patches**
- 6. Manufacturers Are Not Focusing On Identity Theft**

# **DARK WEB**

- 1. Hidden From Search Engines**
- 2. IP Addresses Are Hidden**
- 3. Holds Stolen Financial And Private Data**
- 4. Hard To Track Where Information Is Coming From**



# **DIGITAL ASSISTANTS**

- 1. Amazon Echo, Google Home, Apple SIRI**
- 2. Voice Is Recorded**
- 3. Location Identification**
- 4. Listens To Conversations For “Catch Word”**
- 5. Uncertainty About What Data Is Stored**

# **RANSOMWARE**

- 1. Computer Virus Holds Your Computer Data Hostage**
- 2. Usually Occurs When User Clicks On A Link**
- 3. E-mail Could Look Like From Services Providers**
- 4. Threats To Delete The Hard Drive**
- 5. Wannacry Was Ransomware**
- 6. Usually Pay Off In Bitcoin**
- 7. Important To Keep Back-ups Of Hard Drive**

# **CHIPS IN CREDIT CARDS**

- 1. Chip Holds Payment Data**
- 2. Unique Code For Each Purchase**
- 3. Merchants Liable For Fraudulent Transactions After October 1, 2015**
- 4. Before The Chips, Financial Institutions Handled This Cost Of Fraudulent Transactions**
- 5. Retailer Needs To Buy New Machine And Software.**

# **SOCIAL MEDIA**

- 1. Facebook, LinkedIn, Youtube, Pinterest, Etc.**
- 2. Websites Collect Personal Information**
- 3. Default Privacy Settings Should Be Reviewed**
  - a. Who Can View Your Information**
  - b. Public Information Versus Private**
- 4. Location Postings**
- 5. Create Duplicate Account In Your Name**

# **FAIR CREDIT REPORTING ACT (FCRA)**

**FCRA Provides The Following Rights:**

- 1. Request Fraud Alert**
- 2. Free Copies Of Information On Credit Report**
- 3. Obtain Documents Relating To Fraudulent Transactions**
- 4. Obtain Information From A Debt Collector**
- 5. Ask Credit Reporting Company To Block Information From Identity Theft**
- 6. Prevent Businesses Reporting Information Related To Identity Theft**

# QUESTIONS AND ANSWERS

The image features the text "Q&A" in a 3D, blocky font. The letters "Q" and "A" are a vibrant red, while the ampersand "&" is a metallic grey. The characters are positioned on a white surface, casting soft, light grey shadows beneath them, which gives them a three-dimensional appearance. The overall style is clean and modern.

# CONTACT INFORMATION



**Legend Financial Advisors, Inc.<sup>®</sup>**

5700 Corporate Drive, Suite 350

Pittsburgh, PA 15237-5829

Phone: (412) 635-9210

E-mail: [legend@legend-financial.com](mailto:legend@legend-financial.com)

[www.legend-financial.com](http://www.legend-financial.com)