AVOIDING IDENTITY THEFT

Best Practices Checklist to Prevent Identity Theft

✓ ***Review your Consumer Credit Reports annually***

Request a free copy of your credit reports www.annualcreditreport.com or 1-877-322-8228

✓ ***Opt out of Pre-Approved Credit Cards***

www.optoutprescreen.com or 1-888-5-OPTOUT (1-888-567-8688)

✓ ***Opt out of Junk Mail***

Direct Marketing Association www.dmachoice.org or 1-212-768-7277

✓ ***Opt out of Online Marketing***

Unsubscribe from marketing emails you do not wish to receive by selecting the "unsubscribe" link at the bottom of the email
Direct Marketing Association www.ims-dm.com/cgi/optoutemps.php

✓ ***Opt out of Telemarketing***

Get on the National Do-Not-Call Registry www.donotcall.gov or 1-888-382-1222

✓ ***Safeguard Your Information:***

- Freeze your credit at all four credit reporting agencies. Note: once your credit is frozen, you will need to contact the credit reporting agencies again before you can open any new credit accounts.

  Equifax: https://www.equifax.com/personal/credit-report-services/credit-freeze/

  Experian: https://www.experian.com/freeze/center.html

  TransUnion: https://freeze.transunion.com/sf/securityFreeze/landingPage.jsp

  Innovis: https://www.innovis.com/personal/securityFreeze

- Enable two-factor authentication on all financial accounts, whenever possible
- Do not click on spam or other unknown links or attachments in emails, even if it appears to be coming from a trusted company or person
- Annually request your credit report from all three credit reporting agencies
- Close credit card accounts that you no longer use. However, keep your oldest card active, as closing it can have a particularly negative effect on your credit score
- Passwords on accounts should be at least 12-15 characters with at least one lowercase letter, one uppercase letter, one number and one symbol
- Do not "save" passwords on your web browser
- Do not reuse the same password or PIN for multiple accounts

SilverOak
WEALTH MANAGEMENT LLC

- Maintain up-to-date firewalls, antivirus software and anti-spyware software on all computers
- Ensure that your home router is password protected and you are not using the factory-supplied password
- Make sure all of your devices have up-to-date operating systems, including your smart phones
- Do not email unsecured files with sensitive personal information
- Avoid using public unsecured Wi-Fi
- Have conversations with children about accessing online information through the home network and setting up parental controls when installing new software
- Shred unwanted documents that contain personal information
- Do not send outgoing mail in an unsecured mailbox
- If traveling, have mail held at your local post office usps.com/manage/hold-mail.htm
- If traveling outside of the US, notify credit card companies
- Consider enrolling in Informed Delivery with the US Postal Service by going to http://www.usps.com/manage/informed-delivery.htm
- NEVER give personal information or passwords over the phone, email, or the internet unless you initiated contact
- To prevent someone else from filing a fraudulent tax return, request an IP (Identity Protection) PIN from the IRS irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin
- If your county has a deed alert notifications program, register your property so you will be notified if someone tries to register fraudulent changes to your deed
- Protect your SSN, passwords, PINs and other personal information
- Carry a copy of your Medicare card with your SSN blacked out, only carry your actual Medicare card if your medical provider requests it
- Lock your computer when you are done using it
- Encrypt your data before sending it electronically
- Do not carry your SSN or passwords with you
- Do not put your driver's license number or SSN on your checks
- Review bank statements and credit card statements for accuracy
- Maintain careful records of your bank and financial accounts
- Keep all personal financial records in locked cabinets
- Report lost or stolen credit cards to the issuer immediately
- Review your explanation of medical benefits for fraud

How to tell if you have been a victim of Identity Theft

- There are unexplained withdrawals from your bank account
- Bills or other mail you are expecting do not arrive
- You receive a call from debt collectors about debts that are not yours
- Unfamiliar accounts appear on your credit report
- You receive bills from medical providers for services you did not receive
- Your legitimate medical claims are rejected by your health plan because the records show you have reached your benefits limit
- You receive notification from the IRS that more than one tax return was filed in your name or that you have income from a source you do not recognize
- Your information was compromised by a data breach at a company where you do business or have an account
- You are accused of a crime someone else allegedly committed in your name
- You receive notification about unemployment benefits in your name that you didn't apply for

What to do if you are a victim of Identity Theft

Immediately

(1) Place an Initial Fraud Alert and Request Your Credit Reports

Contact the three credit reporting agencies, place a fraud alert and a credit freeze on your accounts* and request copies of your credit reports:

- Equifax: 1-800-525-6285
  https://www.equifax.com/personal/credit-report-services/credit-fraud-alerts/
- Experian: 1-888-397-3742
  https://www.experian.com/fraud/center.html
- TransUnion: 1-800-680-7289
  https://www.transunion.com/fraud-alerts

* Note: Once your credit has been frozen, you will need to contact the credit reporting agencies before you are able to set up any new accounts.

(2) Create an Identity Theft Report

(a) Report Identity Theft to the Federal Trade Commission (FTC)

- Visit www.identitytheft.gov or call 1-877-438-4338 to complete a report, providing as many details as possible
- Save or print your FTC Identity Theft Affidavit

(b) File a police report

- Go to your local police department or the police department where the theft occurred and bring the following documents:
  - A copy of your FTC Identity Theft Affidavit
  - Any other proof of the theft
  - A government issued ID with a photo
  - Proof of your address
- Complete a police report about the theft
- Ask to have a copy or the number of the police report

(3) Take steps with the IRS

(a) Determine whether the identity theft is tax-related

- Tax-related identity theft involves the theft of your social security number to file a fraudulent tax return. Signs of tax fraud involving a stolen social security number include:
  - You are unable to e-file your return because IRS shows that a return has already been filed using your Social Security Number, or the Social Security Number of a dependent.
  - You receive notice from a tax preparation software company that an account in your name has been accessed, created or disabled without your knowledge.
  - You receive an IRS notice regarding activity you don't recognize, such as wages from an unfamiliar employer, taxes owed for a year that you did not earn income, or being assigned an Employer Identification Number (EIN) when you did not apply for one.
- If you believe that a fraudulent tax return has been filed using your Social Security Number, you should complete and submit Form 14039, Identity Theft Affidavit to the IRS: https://www.irs.gov/pub/irs-pdf/f14039.pdf

(b) Request an IRS Identity Protection (IP) PIN

- If the identity theft does not involve your social security number and filing a fraudulent tax return, you can still safeguard your information with the IRS by requesting an IP PIN
  - Apply for an IP PIN via the IRS website: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin
  - Your IP PIN will be required in order to file future tax returns
  - The IP PIN will change every year and the information will be automatically sent to you in the mail every January. The IP PIN can also be found online at your IRS ID.me account
  - If you are the victim of tax-related identity theft as described above, and have submitted Form 14039, Identity Theft Affidavit to the IRS, they will automatically assign you an IP PIN. You will not need to apply for an IP PIN separately.

(4) Review your homeowner's insurance policy to see if it provides identity theft recovery assistance.

(5) Maintain records of all documents and correspondence related to the identity theft.

Next Steps

- ***Review your credit reports at least annually***
- ***Dispute errors with credit reporting agencies***
- ***Ask the credit reporting agencies to block the fraudulent information on your credit report***
- ***Ask businesses who report errors on your credit report to block the information on your credit report***
- ***Dispute any fraudulent ATM, debit card or credit card charges directly with the financial institution***
- ***Report stolen checks directly to your financial institution and ask them to stop payment***
- ***Contact the check verification companies and inform them that your checks were stolen***
  - TeleCheck 1-800-710-9898
  - Certegy, Inc. 1-800-237-3826
- ***Possibly setup new bank accounts***
- ***If your investment accounts have been tampered with:***
  - Contact your advisor, account manager or your broker
  - File a complaint with the SEC at http://www.sec.gov/complaint.shtml
- ***Dispute any debt collections related to your identity theft***
- ***Keep a file of good records***

  In addition to accurate, complete and secure records, always keep correspondence of conversations you have with others regarding your personal finances.

Communication Guidelines

- Government agencies such as the IRS, Social Security Administration, and Medicare will always communicate via written notice first. Unless you've received written communication, or you have reached out to them and requested a call, they will not contact you over the phone
- Government agencies will NEVER do any of the following:
  - Demand immediate payment or threaten arrest for unpaid bills
  - Ask for credit or debit card numbers over the phone
  - Ask for payment via gift cards, prepaid debit cards, or wire-transfers
  - Require that payments be made to non-government parties
  - Leave pre-recorded, urgent or threatening voicemails
  - Text, email or contact you via social media to ask for personal or financial information, payment or log-in information

If you receive an unexpected call from someone who says they are from a government agency, do not give them any information. Hang up immediately.

Additional Resources on Identity Theft

Federal Trade Commission: www.consumer.gov/idtheft

US Secret Service: www.secretservice.gov/investigation/cyber

Department of Justice: www.justice.gov/criminal/fraud/websites/idtheft.html

Federal Deposit Insurance Corporation: www.fdic.gov/consumers

US Postal Inspection Service: www.uspis.gov

Privacy Rights Clearinghouse: www.privacyrights.org

Internal Revenue Service: www.irs.gov/identity-theft-central

Apply for an IRS Identity Protection PIN: irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin

Contact your state's Attorney General at www.naag.org/find-my-ag