

IDENTITY THEFT / SUSPICIOUS ACTIVITY CHECKLIST

1. SPC Financial® recommends you **report any suspicious Identity Theft activity to local law enforcement and request a police report for future use. Make sure to provide as much documented evidence as possible and keep a copy of the report.**
2. **Contact all credit issuers, credit card companies and credit bureaus in writing of any fraudulent accounts and mistaken information.**
3. **Contact the fraud units at the following credit bureaus and request that they place an account flag requiring future verification of credit requests via fraud alert.**

EQUIFAX

(866) 349-5191
www.equifax.com

To Request a 90 day Fraud Alert:

Website: <https://www.alerts.equifax.com>

Mail: Equifax Information Services LLC
P.O. Box 105069, Atlanta, GA 30348

**For fraud alert extensions, complete and submit Extended Fraud Alert Request Form to the address provided on form, via fax or mail.*

EXPERIAN

(888) 397-3742
www.experian.com

To Request a Fraud Alert:

Website: <https://vww.experian.com/fraud>

Mail: Experian, P.O. Box 9701, Allen, TX 75013

TRANSUNION (800) 680-7289

www.transunion.com

To Request a Fraud Alert:

Website: <https://www.transunion.com/fraud-victim-resource/place-fraud-alert>

Mail: TransUnion Fraud Victim Assistance
P.O. Box 2000, Chester, PA 19016

Note: When requesting fraud alert protection be prepared to provide your Social Security number, current and previous address, date of birth, telephone numbers and identity verification (driver's license or Social Security card).

Investment advisory services offered through SPC Financial® (SPC). SPC and Sella & Martinic, LLC (S&M) are not registered broker/dealers and are independent of Raymond James Financial Services, Inc. (RJFS). RJFS & SPC do not provide tax or legal advice. Tax services and analysis are provided by the related firm S&M through a separate engagement letter with clients.



April 2018



© Copyright 2018

IDENTITY THEFT / SUSPICIOUS ACTIVITY CHECKLIST

INNOVIS (800) 540-2505
<https://www.innovis.com>

To Request a Fraud Alert:

Website: <https://www.innovis.com/fraudActiveDutyAlerts>

Mail: Innovis Consumer Assistance, P.O. Box 26, Pittsburgh, PA 15230

- 4.** Contact credit bureaus in writing to remove any inquiries that have been generated due to any fraudulent access.
- 5.** Reaffirm with Credit Bureaus that your Extended Fraud Alert will remain on your credit report for 7 years.
Note: Most fraud alerts expire after a 90 day period.
- 6.** Contact parties who have received your credit report in the last six months and alert them of any disputed, fraudulent or mistaken information.
- 7.** Request a copy of your credit report.
- 8.** Close accounts that you suspect have been compromised or opened fraudulently.
- 9.** Request replacement cards with new account numbers.

FEDERAL TRADE COMMISSION

- 10.** File a complaint with The Federal Trade Commission (FTC).

FEDERAL TRADE COMMISSION (FTC)
(877) IDTHEFT / (877) 438-4338

Online: Go to the website listed below to report identity theft and get a recovery plan. The plan includes the forms, affidavits, and letters you'll need.

<https://www.identitytheft.gov/>

LOCAL POLICE

- 11.** Report the crime to your local police or sheriff's department immediately. Make sure you provide the police with as much documented evidence as possible. You should verify that the police report lists the fraudulent accounts and keep a copy of the report.

IDENTITY THEFT / SUSPICIOUS ACTIVITY CHECKLIST

DEBT COLLECTORS

- 12.** Tell collectors that you are a victim of fraud and are not responsible for the account.
- 13.** Ask for the name of the collection company, the name of the person contacting you, their phone number and their address.
- 14.** Ask for the name and contact information for the referring credit issuer, the amount of the debt, account number and dates of the charges.
- 15.** Ask if the debt collector needs you to complete a specific fraud affidavit form or whether the FTC affidavit may be used.
- 16.** Ensure that you follow up, in writing, with the debt collector and that the debt collector confirms, in writing, that you do not owe the debt and that the account has been closed.

NOTE: Under the Fair Credit Reporting Act (FCRA), a debt collector must notify the creditor that the debt may be a result of identity theft (§615(g)). The FCRA also prohibits the sale or transfer of a debt caused by identity theft (§615(f)).

OTHER IDENTITY THEFT ISSUES

- 17. U.S. mail fraud:** Visit the U.S. Postal Service® Website, Government Services.
Website: <http://postalinspectors.uspis.gov>
Phone: (800) 275-8777
- 18. Financial fraud/fraud ring:** You should contact the U.S. Secret Service.
Website: <http://www.secretservice.gov>
- 19. Social Security number misuse (non-IRS issues):** You should contact the SSA Inspector General to report Social Security benefit fraud, employment fraud, or welfare fraud.
Website: www.socialsecurity.gov/oig
Fraud Reporting:
 - **SSA fraud hotline:** (800) 269-0271
 - **Mail:** Social Security Fraud Hotline, P.O. Box 17785, Baltimore, MD 21235
- 20. Driver's license number fraud:** Notify your state's Department of Motor Vehicles.
- 21. Social Security number used to commit identity theft:** Notify the Federal Trade Commission at **1 (877) ID THEFT** or **<https://www.identitytheft.gov>**.

IDENTITY THEFT / SUSPICIOUS ACTIVITY CHECKLIST

- 22. Passport used in identity theft:** Contact the U.S. State Department, Passport Services Department.
- 23. IRS tax-related identity theft:** Contact the IRS to report the theft and file IRS Form 14039, *Identify Theft Affidavit*.

IRS Identity Protection Specialized Unit (IPSU): (800) 908-4490
Form 14039, Identity Theft Affidavit

NOTE: There are two types of tax-related identity theft – refund theft and employment theft. Refund theft occurs when a thief files a return before you do, and the IRS, unable to detect any issues at the time of filing, erroneously issues a refund to the thief. Employment theft occurs when a thief uses your client's identification number to obtain a job. You should report both types to the IPSU. The IRS will place a flag on the account and monitor it more closely. The IRS will also issue an Identity Protection Personal Identification Number (IP-PIN) each December. Ensure that you file your return using this number. Additional information is available at IRS.gov.

REMINDERS AND CONSIDERATIONS

- 24.** You should create an identity theft file and keep copies of everything.
- 25.** In all communications with the credit bureaus, you should refer to the unique number assigned to your credit report and, when mailing information, use certified, return receipt. Be sure that you save all credit reports as part of the fraud documentation file.
- 26.** File a complaint with the Internet Crime Complaint Center (IC3). The IC3 is a partnership between the Federal Bureau of Investigation (FBI) and the National White Collar Crime Center and works to resolve internet and cyber-crime issues.
Website: <http://www.ic3.gov>
- 27.** Request a security freeze at each of the credit bureaus' websites. By freezing your credit reports, you can prevent credit issuers from accessing credit files. This effectively prevents thieves from opening new credit card and loan accounts.
- 28.** Request free annual credit reports.
Website: <https://www.annualcreditreport.com>
- 29.** Request an extended fraud alert, which allows you to obtain two free credit reports from each of the credit reporting companies within 12 months.

The information has been obtained from sources considered to be reliable, but we do not guarantee that the foregoing material is accurate or complete. Links are being provided for information purposes only. RJFS, SPC and S&M are not affiliated with and do not endorse, authorize or sponsor any of the listed websites or their respective sponsors, and they are not responsible for the content of any referenced website or the collection or use of information regarding any website's users and/or members.