Identity Theft Checklist

Use this checklist to assist you in addressing identity theft issues involving credit agencies, the Federal Trade Commission (FTC), local police, and debt collectors. In addition, this checklist will help you resolve other identity theft problems, including IRS tax-related identity theft.

CREDIT AGENCIES AND CREDIT REPORT REVIEW

1. Report the identity theft to the fraud department of one of the following credit reporting agencies as soon as possible. Then notify the other two agencies.

Equifax – www.equifax.com
Request a 90-day fraud alert:
Online: https://www.alerts.equifax.com/
Phone: (888) 766-0008
Mail: Equifax Consumer Fraud Division, PO Box 740256 Atlanta, GA 30374

*To request an extended fraud alert, complete and submit the Extended Fraud Alert Request Form. Fax or mail it to the address shown on the form.

Experian – www.experian.com/
To add a fraud alert:
Online: Credit Fraud Center
Phone: (888) 397-3742

TransUnion – www.transunion.com/
To add a fraud alert:
Online: https://fraud.transunion.com/
Phone: (800) 680-7289
Mail: TransUnion LLC, P.O. Box 2000, Chester, PA 19022-2000

NOTE: Be prepared to provide your Social Security number, current and previous address, date of birth, telephone number, and identity verification, such as a copy of a driver's license or Social Security card.

2. Request a copy of your credit report.

3. Close accounts that you think have been compromised or opened fraudulently.

4. Inform the credit bureaus and the credit issuers (in writing) of any fraudulent accounts and mistaken information.

5. Request replacement cards with new account numbers.

6. Contact the credit bureaus (in writing) to remove any inquiries that have been generated due to the fraudulent access.

7. Notify those who have received your credit report in the last six months to alert them of any disputed, fraudulent, or mistaken information.

8. Confirm that an extended fraud alert (7 years) is placed on the credit report.

NOTE: Often, you will put an initial 90-day fraud alert on the account and later need the longer alert period.

FEDERAL TRADE COMMISSION (FTC)

9. File a complaint with the FTC and obtain a copy of the Identity Theft Affidavit for your records.

Online resources:
Identity Theft Victim's Complaint and Affidavit
Create an Identity Theft Report
Phone: (877) IDTHEFT [(877) 438-4338]
Mail: FTC Identity Theft Clearinghouse, 600 Pennsylvania Ave. N.W. Washington, DC 20580

NOTE: Developed by the FTC in conjunction with banks, credit grantors, and consumer advocates, the FTC's Identity Theft Affidavit is accepted by participating credit issuers, retailers, banks, and other financial institutions. The FTC's Identity Theft Affidavit is separate and distinct from the IRS' Form 14039, Identity Theft Affidavit, which is used to report tax-related identity theft to the IRS.

LOCAL POLICE

10. Report the crime to your local police or sheriff's department right away. Make sure you give the police as much documented evidence as possible. You should then verify that the police report lists the fraudulent accounts and keep a copy of the report.

DEBT COLLECTORS

11. Tell collectors that you are a victim of fraud and are not responsible for the account.

12. Ask for the name of the collection company/the name of the person contacting you, the phone number, and the address.

13. Ask for the name and contact information for the referring credit issuer, the amount of the debt, account number and dates of the charges.

14. Ask if the debt collector needs you to complete a specific fraud affidavit form or whether the FTC affidavit may be used.

15. Follow up, in writing, with the debt collector and ensure 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

16. **U.S. mail fraud:** Contact your local Postal Inspector.
Online: http://postalinspectors.uspis.gov/

Phone: (800) 275-8777

17. **Financial fraud/fraud ring:** Contact the U.S. Secret Service.
Online: http://www.secretservice.gov/criminal.shtml

18. **Social Security number misuse – non-IRS issues:** Contact the SSA Inspector General to report Social Security benefit fraud, employment fraud, or welfare fraud.

Online resources: www.socialsecurity.gov/oig
Fraud Reporting Form
SSA fraud hotline: (800) 269-0271
Mail: Social Security Fraud Hotline, P.O. Box 17785, Baltimore, MD 21235

19. **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 identification number to obtain a job. You should report both types to the IPSU. The IRS will place a maker 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 your number. Additional information is available at www.IRS.gov.

REMINDERS AND CONSIDERATIONS

20. You should create an identity theft file and keep copies of everything.

21. 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.

22. Consider filing 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/default.aspx

23. Consider requesting a security freeze. By freezing your credit reports, you can prevent credit issuers from accessing credit files (except when you give specific permission). This effectively prevents thieves from opening new credit card and loan accounts.
More information: http://www.consumeraction.org/english/articles/freeze_your_credit_file#Topic_04

24. Consider obtaining free annual credit reports. Website: https://www.annualcreditreport.com/cra/index.jsp

25. Consider requesting an extended fraud alert, which allows you to obtain two free credit reports from each of the credit reporting companies within 12 months.

Disclosure

This communication and its content are for informational and educational purposes only and should not be used as the basis for any investment decision. The information contained herein is based on publicly available sources believed to be reliable but is not a representation, expressed or implied, as to its accuracy, completeness or correctness. No information available through this communication is intended or should be construed as any advice, recommendation or endorsement from us as to any legal, tax, investment or other matters, nor shall be considered a solicitation or offer to buy or sell any security, future, option or other financial instrument or to offer or provide any investment advice or service to any person in any jurisdiction. Nothing contained in this communication constitutes investment advice or offers any opinion with respect to the suitability of any security, and this communication has no regard to the specific investment objectives, financial situation and particular needs of any specific recipient. Past performance is no guarantee of future results. Additional information and disclosure on Pathstone is available via our Form ADV, Part 2A, which is available upon request or at www.adviserinfo.sec.gov.

Any tax advice contained herein, including attachments, is not intended or written to be used, and cannot be used, by a taxpayer for the purpose of (i) avoiding tax penalties that may be imposed on the taxpayer or (ii) promoting, marketing or recommending to another party any transaction or matter addressed herein.