IDENTITY THEFT – STEPS TO CONSIDER

CREDIT AGENCIES AND CREDIT REPORT REVIEW

Report the identity theft to the fraud department to ONE of the following credit reporting agencies, as soon as possible. ***They*** must notify the other two agencies.

- **Equifax** – www.equifax.com
  Request a 90-day fraud alert:
  - Online: https://www.alerts.equifax.com/
    (More online information)
  - 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. You should fax or mail it to the address shown on the form.
- **Experian** – www.experian.com/
  To add a fraud alert:
  - Online: Credit Fraud Center
    (More online information)
  - Phone: (888) 397-3742
- **TransUnion –** www.transunion.com/
  To add a fraud alert:
  - Online: https://fraud.transunion.com/
    (More online information)
  - 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.

Request a copy of your credit report.

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

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

Request replacement cards with new account numbers.

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

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

Confirm that an extended fraud alert (7 years) is placed on the credit report. *An initial 90-day fraud alert on the account is standard, but you may find you need the longer alert period.*

FEDERAL TRADE COMMISSION (FTC)

File a complaint with the FTC.

- 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. Contact your CPA should you want this form also submitted (in addition to the IRS affidavit).

LOCAL POLICE

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

DEBT COLLECTORS

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

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

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

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

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

U.S. mail fraud: You should contact your local Postal Inspector.

- Online: http://postalinspectors.uspis.gov/
- Phone: (800) 275-8777

Financial fraud/fraud ring: contact the U.S. Secret Service.

- Online: http://www.secretservice.gov/criminal.shtml

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

REMINDERS AND CONSIDERATIONS

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

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.

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

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.consumer-action.org/english/articles/freeze_your_credit_file#Topic_04

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

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.