



Identity Theft Victim Procedures

Bensalem Township Police Department

Criminal Investigation Division

2400 Byberry Rd.

Bensalem, PA 19020

215-633-3700

www.bensalempolice.org

Identity Theft: Victim Procedures- There are six main steps victims should take upon discovering that they are a victim of an identity crime. The steps are: File a police report; Obtain and complete a copy of the Identity Theft Affidavit; Close all compromised accounts; Place a fraud alert with the credit bureaus; Request that credit reporting bureaus block fraudulent information; and File a complaint with the Federal Trade Commission.

File a police report- Victims are required to file a police report in order to dispute fraudulent transactions, correct compromised accounts, place fraud alerts with the credit bureaus and to obtain free copies of their credit reports to review.

Victims should obtain and retain a copy, receipt, or summary of the initial police report. The Fair & Accurate Credit Transaction Act requires law enforcement to provide victims of identity theft with a copy of the police report.

Note- While the FACT Act and the Fair Credit Reporting Act stipulates that a copy of an official police report be provided to victims of identity theft, some Pennsylvania police departments will not issue an actual report to a victim, but rather a report summary, or perhaps only the report number. Since the police report, or summary becomes the official basis upon which a victim can dispute identity crime related fraud by establishing that they are in fact a victim of identity fraud, a copy of, or access to this document must be ensured.

The victim will need to send a copy of the initial police report to each involved bank, creditor, other business, credit bureau, and debt collector in order to dispute compromised or fraudulent accounts or transactions. A copy of this report, summary, or report number must be coupled with each affidavit.

The victim should be told to keep an original copy of the report, but copy it as many times as necessary.

The victim should keep a detailed journal to record every corrective action, all names of companies or representatives to whom they speak or write, what victims have been told and who told them. The victim should record any action they take during this process.

Obtain & complete an Identity Theft Affidavit for each compromised or fraudulently opened account- The victim is required to prepare an affidavit stating they did not commit the fraud.

Note- A copy of an Identity Theft Affidavit that is accepted by most businesses, creditors and debt collectors, and that can be obtained at the Federal Trade Commission website <http://www.consumer.gov/idtheft/> is provided in Appendix C.

In order to dispute a fraudulent account or transaction, a *copy* of this affidavit must be coupled with a copy of the police report, report summary, or report number, and sent to every creditor, business, and debt collector through which a fraudulent account or transaction has occurred.

Close all accounts believed to have been compromised or opened fraudulently- Victims should immediately contact their credit card companies, banking and other financial institutions, and close all accounts that may have been compromised or subjected to a fraudulent take-over by unauthorized persons. Victims can work with their financial institution(s) to re-establish an alternate account to prevent further fraud or compromise.

After a thorough review of their credit report, (see next section,) victims should close all accounts that were opened fraudulently, opened without their knowledge, or that display suspicious activity.

Place a fraud alert with each credit bureau; obtain and review credit reports- Victims must contact at least one credit bureau to place a fraud alert. The victim will then receive free credit reports from all three credit bureaus in order to identify new fraudulent activity or compromised accounts.

Note- The Fair Credit Reporting Act requires each major nationwide credit bureau to provide consumers with a free annual credit report which can be obtained through www.annualcreditreport.com

a. **Credit Bureaus-** The three major credit bureaus are:

- ◆ Equifax - www.equifax.com
P.O. Box 740241, Atlanta, GA 30374-0241
800-525-6285
- ◆ Experian - www.experian.com
P.O. Box 9530, Allen, TX 75013
888-EXPERIAN (397-3742)
- ◆ Trans Union - www.transunion.com
Fraud Victim Assistance Division,
P.O. Box 6790, Fullerton, CA 92634
800-680-7289

Fraud Alerts- Victims can place a fraud alert on their credit report in order to prevent the opening of additional fraudulent accounts and to flag additional fraudulent activity.

Federal law requires that when a victim informs a credit bureau of a compromised account, that credit bureau must inform the remaining credit bureaus of the fraud alert. However, some incidents have been reported in which the victim was required to contact the remaining credit bureaus in order to place a fraud alert with each of the remaining bureaus.

Fraud alerts require an entity or business to verify a person's identity before issuing credit.

Types of Fraud Alerts- There are two types of fraud alerts, an Initial and an Extended Alert.

Initial Fraud Alerts- An initial fraud alert is active on a victim's credit report for at least 90 days.

- Placement of this type of alert on a credit report requires providing appropriate proof of the victim's identity, including SSN, name, address, and other personal information.
- Placement of an initial fraud alert entitles a victim to obtain one free credit report from each of the three national consumer reporting companies.
- Initial fraud alerts are automatically placed on a compromised account upon report from a victim.

Extended Fraud Alerts- An extended fraud alert is active for seven years, and entitles the victim to receive two free credit reports within 12 months from each of the three national consumer reporting companies.

- Upon placement of an extended fraud alert, consumer reporting companies will also remove the victim's name from the list of pre-screened credit offers for five years.
- In most cases, victims must request an extended fraud alert be placed on their accounts.

Credit reporting companies; blocking fraudulent information from credit report- The Fair Credit Reporting Act establishes procedures for correcting fraudulent information on the victim's credit reports and requires that the victim's credit report be made available only for certain legitimate business needs.

Under the FCRA, both the consumer reporting company and the information provider (the business such as a bank or credit card company that sent the information to the consumer reporting company), are responsible for correcting fraudulent information in the victim's report. To protect the victim's rights under the law, the victim needs to contact both the consumer reporting company and the information provider.

Consumer reporting companies will block fraudulent information from appearing on the victim's report if the victim sends them a copy of the police report and a letter telling them what information is fraudulent. The letter also should state that the information does not relate to any transaction that the victim made or authorized. In addition, victims must provide proof of their identity that may include their SSN, name, address, and other personal information requested by the consumer reporting company.

The consumer reporting company has four business days to block the fraudulent information after accepting the victim's police report and letter. It also must tell the information provider that it has blocked the information.

The consumer reporting company may refuse to block the information or remove the block; if for example, the victim has not told the truth about their identity theft. If the consumer reporting company removes the block or refuses to place the block, it must inform the victim.

File a complaint with the Federal Trade Commission - The victim should file a complaint with Federal Trade Commission Identity Theft Hotline at 1-877-438-4338 or on the internet at www.consumer.gov/idtheft . Information pertaining to the theft or misuse of identifying information is entered into the Hotline database. This information is then processed into the Consumer Sentinel Database that is available to law enforcement officers.

Identity Theft: Police Procedures- U.S. Congress criminalized identity theft under the Identity Theft and Assumption Deterrence Act of 1998. Under this act the Federal Trade Commission was required to establish a consumer education service and a centralized data base of victim complaints for law enforcement to use in tracking cases and defendants.

SECURITY FREEZE INFORMATION

Any consumer in Pennsylvania may place a security freeze on his or her credit report by requesting one in writing by certified mail to the credit reporting agency. The credit reporting agency is not allowed to charge a fee to victims or seniors 65 years of age or older for placing, removing for a specific period or party, or removing a security freeze on a credit report. To avoid a fee, the victim must send a valid copy of a police report to the credit reporting agency. However, for other consumers, a charge of \$10 will be applied for each placing or temporary lifting of a security freeze. There is no fee to remove the freeze. A security freeze shall prohibit, with certain specific exceptions, the credit reporting agency from releasing the consumer's credit report or any information from it without the express authorization of the consumer. The freeze goes into effect five (5) business days from receipt of the consumer's letter by the credit reporting agency.

To obtain more detailed information on how to place a security freeze on your credit reports, see below.

HOW TO "FREEZE" YOUR CREDIT FILES

A security freeze means that your file cannot be shared with potential creditors. A security freeze can help prevent identity theft. Most businesses will not open credit accounts without checking a consumer's credit history first. If your credit files are frozen, even someone who has your name and Social Security number probably would not be able to obtain credit in your name. A security freeze is free to identity theft victims who have a police report. A freeze on your account is good for 7 years in Pennsylvania.

How do I place a security freeze?

To place a freeze, you must send by certified mail a letter to each consumer reporting agency requesting a security freeze be placed on your account. In this letter you must provide identifying information and a \$10 fee, but, if you are a victim or, you must also include a copy of your police report to avoid a charge paying a \$10 fee. Seniors who are at least 65 years old also do not need to pay to place a security freeze. (In the future, it will be possible to place a freeze through a secure electronic connection—likely by sending an e-mail on the consumer reporting agency's website.)

Write to all three addresses below and include the information that follows:

Equifax Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Trans Union Security Freeze
P.O. Box 6790

Fullerton, CA 92834-6790

For each, you must:

- Send a letter by certified mail;
- If you are a victim, include a copy of your the police report concerning identity theft;
- Provide your full name (including middle initial as well as Jr., Sr., II, III, etc.,) address, Social Security number, and date of birth;
- If you have moved in the past 5 years, supply the addresses where you have lived over the prior 5 years.
- Provide proof of current address such as a current utility bill or phone bill
- Send a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
- If applicable, include a payment by check, money order or credit card (Visa, Master Card, American Express, and Discover cards only.)

How long does it take for a security freeze to be in effect?

After five (5) business days from receiving your letter, the credit reporting agencies listed above will place a freeze providing credit reports to potential creditors.

After 10 business days from receiving your letter to place a freeze on your account, the credit reporting agencies will send you a confirmation letter containing a unique PIN (personal identification number) or password. Keep this PIN or password in a safe place.

Can I open new credit accounts if my files are frozen?

Yes. You can have a security freeze lifted for a temporary period of time or with a specific creditor. The steps to do so are as follows:

- Contact the credit reporting agencies above by certified mail or by a toll-free phone number they are required by law to create.
- You must provide proper identification;
- You must provide your unique PIN or password; AND
- To lift the freeze for a period of time, you must provide the time period your credit report will be accessible to third parties OR to lift for a specific creditor, you must indicate which creditor you will grant access to your credit files.

How long does it take for a security freeze to be lifted?

Credit bureaus must lift a freeze no later than three (3) business days from receiving your request.

What will a creditor who requests my file see if it is frozen?

A creditor will see a message or a code indicating the file is frozen.

Can a creditor get my credit score if my file is frozen?

No. A creditor who requests your file from one of the three credit bureaus will only get a message or a code indicating that the file is frozen.

Can I order my own credit report if my file is frozen?

Yes.

Can anyone see my credit file if it is frozen?

When you have a security freeze on your credit file, certain entities still have access to it. Your report can still be released to your existing creditors or to collection agencies acting on their own behalf. They can use it to review or collect on your account. Other creditors may also use your information to make offers of credit. Government agencies may also have access in response to a court or administrative order, a subpoena, or a search warrant.

Do I have to freeze my file with all three credit bureaus?

Yes. Different credit issuers may use different credit bureaus. If you want to stop your credit file from being viewed, you must freeze it with Equifax, Experian, and Trans Union.

Will a freeze lower my credit score?

No.

Can an employer do a background check on my credit file?

No. You would have to lift the freeze to allow a background check, just as you would to apply for credit. The process for lifting the freeze is described above.

How long will a security freeze be in effect?

A security freeze will end after 7 years from the date you placed it.

Does freezing my file mean that I won't receive pre-approved credit offers?

No. You can stop the pre-approved credit offers by calling 888-5OPTOUT (888-567-8688). Or you can do this online at www.optoutprescreen.com. This will stop most of the offers, the ones that go through the credit bureaus. It's good for five years or you can make it permanent.

What law requires security freezes?

The law on security freezes in Pennsylvania passed as Senate Bill 180.

THIS FACT SHEET IS FOR INFORMATIONAL PURPOSES AND SHOULD NOT BE CONSTRUED AS LEGAL ADVICE OR AS THE POLICY OF THE STATE OF PENNSYLVANIA. IF YOU WANT ADVICE ON A PARTICULAR CASE, YOU SHOULD CONSULT AN ATTORNEY OR OTHER EXPERT. THE FACT SHEET MAY BE COPIED, IF (1) THE MEANING OF THE COPIED TEXT IS NOT CHANGED OR MISREPRESENTED, (2) CREDIT IS GIVEN TO THE OFFICE OF THE PENNSYLVANIA ATTORNEY GENERAL, AND (3) ALL COPIES ARE DISTRIBUTED FREE OF CHARGE.

Before using these template letters, please read the entire document for complete information.

SAMPLE FREEZE LETTER TO EQUIFAX

Date

Equifax
Security Freeze
P.O. Box 105788
Atlanta, GA 30348

Dear Equifax:

I would like to place a security freeze on my credit file. My name is:

My former name was (if applies):

My current address is:

My address has changed in the past 5 years. My former address was:

My social security number is:

My date of birth is:

I have enclosed photocopies of a government issued identity card AND proof of residence such as a utility bill or phone bill.

Circle one:

I have included my payment of \$10 (or however much increased by the CPI) to freeze my credit file.

OR

I am an identity theft victim and a copy of my police report of identity theft is enclosed.

OR

I am a senior who is aged 65 years or older.

Yours Truly,

You.

SAMPLE FREEZE LETTER TO TRANS UNION

Date

Trans Union Security Freeze
P.O. Box 6790
Fullerton, CA 92834-6790

Dear Trans Union:

I would like to place a security freeze on my credit file. My name is:

My former name was (if applies):

My current address is:

My address has changed in the past 5 years. My former address was:

My social security number is:

My date of birth is:

I have enclosed photocopies of a government issued identity card AND proof of residence such as a utility bill or phone bill.

Circle one:

I have included my payment of \$10 (or however much increased by the CPI) to freeze my credit file.

OR

I am an identity theft victim and a copy of my police report of identity theft is enclosed.

OR

I am a senior who is aged 65 years or older.

Yours Truly,

Your name

SAMPLE FREEZE LETTER TO EXPERIAN

Date

Experian Security Freeze
P.O. Box 9554
Allen, TX 75013

Dear Experian:

I would like to place a security freeze on my credit file. My name is:

My former name was (if applies):

My current address is:

My address has changed in the past 5 years. My former address was:

My social security number is:

My date of birth is:

I have enclosed photocopies of a government issued identity card AND proof of residence such as a utility bill or phone bill.

Circle one:

I have included my payment of \$10 (or however much increased by the CPI) to freeze my credit file.

OR

I am an identity theft victim and a copy of my police report of identity theft is enclosed.

OR

I am a senior who is aged 65 years or older.

Yours Truly,

Your name

IDENTITY THEFT

In order to better protect yourself, it is helpful to know some of the ways identity thefts can occur. Thieves:

- Steal wallets and purses containing personal identification and credit/bank cards.
- Steal mail, including bank and credit card statements, pre-approved credit offers, new checks and tax information
- Complete a change of address form to divert mail to another location.
- Rummage through trash, or the trash of businesses, for personal data in a practice known as "dumpster diving"
- Find personal information in homes
- Use personal information individuals share on the Internet
- Send e-mail posing as legitimate companies or government agencies with which individuals do business.
- Get information from the workplace in a practice known as "business record theft" by stealing files out of offices where a person is a customer, employee, patient or student, bribing an employee who has access to personal files, or "hacking" into electronic files.

HOW TO AVOID IDENTITY THEFT

All consumers should take the following steps to prevent identity theft from occurring:

- Review Credit Reports from each of the three major credit bureaus once a year.
- Place passwords on your credit card, bank and phone accounts.
- Secure personal information in your home.
- Ask about information security procedures in your workplace.
- Don't carry your social security card with you; leave it in a secure place.
- Don't give out your social security number unless it is absolutely necessary; ask to use other types of identifiers when possible.
- Don't give out personal information over the phone, through the mail or over the internet unless you have initiated the contact or are sure you know with whom you are dealing.
- Guard your mail and trash from theft.
- Destroy offers of credit received in the mail that you do not respond to; you may choose to opt-out of receiving free offers of credit.
- Carry only the identification information and the number of credit/debit cards that you actually need.
- Pay attention to your billing cycles—follow up with creditors if bills do not arrive on time.
- Be wary of promotional scams.
- Keep your purse or wallet in a safe place at work.
- Notify your credit card company if you are planning to travel out of state.

WHAT TO DO IF YOU ARE A VICTIM OF IDENTITY THEFT

If you are a victim of identity theft, or believe you may be a victim, it is important that you take the following steps:

- Place a fraud alert on your credit reports and review your credit reports
- Place a security freeze on your credit reports.
- Close any accounts that have been tampered with or opened fraudulently.
- File a police report and ask for a copy for your records
- File a complaint with the Federal Trade Commission and the Attorney General's Office.
- Write down the name of anyone you talk to, what s/he told you, and the date of the conversation.
- Follow-up in writing with all contacts you have made about the identity theft on the phone or in person. Use certified mail, return receipt requested, for all correspondence regarding identity theft.
- Keep all copies of all correspondence or forms relating to identity theft.
- Keep the originals of supporting documentation, like police reports and letters to and from creditors; send copies only.
- Keep old files, even if you believe the problem is resolved. If it happens again, you will be glad you did.