MEMBER
IDENTITY THEFT GUIDANCE SHEET

This document is a brief summary of the best practices related to identity theft. Comprehensive action steps are detailed through the resources cited in this summary. It is not the intent of PTF Federal Credit Union, or any of its employees, to provide legal counsel to members or consumers who feel they may have been a victim of identity theft.

INTRODUCTION

Identity theft happens when someone steals your personal information and uses it without your permission. It is a serious crime that can wreak havoc with your finances, credit history, and reputation – and it can take time, money, and patience to resolve.

If you suspect that someone has stolen your identity, acting quickly is the best way to limit the damage. Setting things straight involves some work.

How do thieves get my information?

"I thought I kept my personal information safe!"

You may be very careful with your personal information, but identity thieves are resourceful and use a variety of ways to get your information. They may "dumpster dive" or rummage through your garbage, the trash of business, or public dumps. They may take mail from your mailbox. They may work for, or pretend to work for, legitimate companies, medical offices, clinics, pharmacies, or government agencies. Then they may take advantage of that role to convince you to reveal personal information. Some thieves pretend to represent an institution you trust and try to trick you by email or phone into revealing personal information.

How do I protect my child's identity?

A child's Social Security number can be used by identity thieves to apply for government benefits, open bank and credit card accounts, apply for a loan or utility service, or rent a place to live. Determine if there is credit report in your child's name; to see if your child's information is being misused. Take immediate action if it is.

Many school forms require personal and, sometimes, sensitive information. Find out how your child's information is collected, used, stored, and thrown away. Your child's personal information is protected by law. Asking schools and other organizations to safeguard your child's information can help minimize your child's risk of identity theft.

The Federal Family Educational Rights and Privacy Act (FERPA), enforced by the U.S. Department of Education, protects the privacy of student records. It also gives parents of school-age kids the right to opt-out of sharing contact or other directory information with third parties, including other families.

It's a good idea to check whether your child has a credit report close to the child's 16th birthday. If there is one and it has errors due to fraud or misuse, you will have time to correct it before the child applies for a job, a loan for tuition or a car, or needs to rent an apartment.

What do thieves do with my information?

Once identity thieves have your personal information, they can drain your bank account, run up charges on your credit cards, open new utility accounts, or get medical treatment on your health insurance. An identity thief might even file a tax return in your name and get your refund. In some extreme cases, a thief might even give your name to the police during an arrest.

Some identity thieves use your information right away. Some will hold the information for a while then begin using it. Some identity thieves "sell" your information on the black market.

How can I tell that someone has stolen my information?

These are some of the signs to watch for:

- You see unexplained withdrawals from your bank account
- You do not get your bills or other mail
- Merchants refuse to take your checks
- Debt collectors call you about debts that are not yours
- You find unfamiliar accounts or charges on your credit report
- Medical providers bill you for services that you did not use
- Your health plan rejects your legitimate medical claim because their records show you have reached your benefits limit
- The Internal Revenue Service notifies you that more than one tax return was filed in your name
- The Internal Revenue Service notifies you that you have income from an employer you do not know
- You get notice that your information was compromised by a data breach at a company where you do business or have an account
- You are arrested for a crime someone else allegedly committed in your name

What should I do if my information is lost or stolen, but my accounts do not show any problems?

If your wallet, Social Security card, or other personal, financial, or account information is lost or stolen, contact the credit reporting companies and place a fraud alert on your credit file. Check your credit union, bank, and other statements for unusual activity. You may want to take additional steps, depending on what information was lost or stolen. You can exercise your legal right to a free copy of your credit report.

If your information is lost in a data breach, the organization involved in the breach will notify you and tell you about your rights. Generally, you may choose to:

- Place a fraud alert on your credit file
- Monitor your accounts for unusual activity
- Exercise your right to a free copy of your credit report

You may have other rights under state law.

Where do I turn for help?

There are multiple, free resources available for consumers who have been, or think they have been, a victim of identity theft.

It is not the intent of PTF Federal Credit Union to provide any legal counsel to members or consumers who feel they may have been a victim of identity theft.

A good place to start is with the Federal Trade Commission.

Federal Trade Commission (FTC)

- www.FTC.gov/IDTheft
- By phone at 877-438-4338 or 866-653-4261 (TTY)

Other resources include the CFPB and the State Attorney General for the State in which you reside.

Consumer Financial Protection Bureau (CFPB)

- www.consumerfinance.gov then search for "Identity Theft"
- By phone at 855-411-2372

Indiana Attorney General for Indiana residents

- http://www.in.gov/attorneygeneral/ then search for "Identity Theft"
- By phone at 800-382-5516

Consumers should be cautious of "credit repair" companies that offer to "fix credit" or "repair your life" after you have become a victim of identity theft.

What are my first steps?

1. **Contact any one of the nationwide consumer reporting companies** to place an initial fraud alert on your credit report. Fraud alerts can help prevent an identity thief from opening any more accounts in your name.

Placing a fraud alert is free. The initial fraud alert stays on your credit report for 90 days. Be sure the credit reporting company has your current contact information so they can get in touch with you.

The company you call is required to contact the other two, which will place an alert on their versions of your report.

- TransUnion: 1-800-680-7289
- Equifax: 1-800-525-6285
- Experian: 1-888-397-3742

- Report that you are an identity theft victim
- Ask the company to put a fraud alert on your credit file
- Confirm that the company you call will contact the other two companies.

When you have a fraud alert on your credit report, a business must verify your identity before it issues credit in your name.

2. **Order your Credit Reports** after you place an initial fraud alert, the credit reporting company will explain your rights and how you can get a copy of your credit report.

Placing an initial fraud alert entitles you to a free credit report form each of the three credit reporting companies

Contact **each** credit reporting company:

- TransUnion: 1-800-680-7289
- Equifax: 1-800-525-6285
- Experian: 1-888-397-3742

- Explain you placed an initial fraud alert
- Order your free copy of your credit report
- Ask each company to show only the last 4 digits of your Social Security number on your report
- Record the dates you made the calls or sent letters
- Keep copies of letters in your files

Contact the security or fraud department of each company where you know, or believe, accounts have been tampered with or opened fraudulently. Close the accounts. Follow up in writing, and include copies (NOT originals) of supporting documents.

Each company might have different requirements to initiate the investigation of identity theft.

It's important to notify credit card companies and banks in writing. Send your letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures. When you open new accounts, use new Personal Identification Numbers (PINs) and passwords. Avoid using easily available information like your mother's maiden name, your birth date, the last four digits of your Social Security number or your phone number, or a series of consecutive numbers.

> ***PTF Federal Credit Union requires that Member notify us in a handwritten statement if they feel they have been a victim of identity theft. Statement must be signed and dated by all account holders.***

3. **Create an Identity Theft Report** which helps you deal with credit reporting companies, debt collectors, and businesses that opened accounts in your name. You can use the Report to:

- Get fraudulent information removed from your credit report
- Stop a company from collecting debts that result from identity theft or from selling the debt to another company for collection
- Place an extended fraud alert on your credit report
- Get information from companies about accounts the identity thief opened or misused

Creating an Identity Theft Report involves 3 steps:

1. Submit a complaint about the theft to the FTC. When you finish writing all the details, print a copy of the report. It will print as an "Identity Theft Affidavit."
2. File a police report about the identity theft and get a copy of the police report or the report number. Bring your FTC Identity Theft Affidavit when you file a police report
3. Attach your FTC Identity Theft Affidavit to your police report to make an "Identity Theft Report."

Some companies want more information than the Identity Theft Report includes. Some companies want different information. The information you need to provide depends on the policies of the credit report company and the business that sent the information about you to the credit reporting agency.

PTF requires a copy of the Police report be provided within three (3) business days of initial notification of identity theft in addition to the handwritten statement.

It is not the intent of PTF Federal Credit Union to provide any legal counsel to members or consumers who feel they may have been a victim of identity theft.