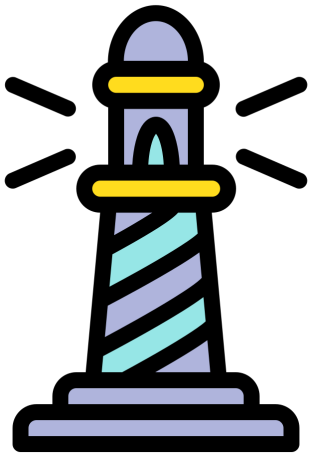


SecurityPamphlet.com

IDENTITY THEFT
PAMPHLET 01

ver 1.1

May 2024

AUTHOR: DURGESH KALYA, CISSP
questions@SecurityPamphlet.com

Fine Print:

This document is intended for individuals looking for an introduction to the subject of the intended topic and should not be used as professional advice or in place of a professional service. Now you have been warned.

What is Identity Theft?

Identity theft occurs when someone unlawfully obtains and uses another person's personal information for fraudulent purposes. This stolen information can include Social Security numbers, credit card details, bank account numbers, and other sensitive data. Perpetrators of identity theft can use this information to open fraudulent bank accounts, apply for loans or credit cards, make purchases, or even commit crimes in the victim's name. The consequences of identity theft can be severe, including financial loss, damage to credit scores, legal issues, and emotional distress for the victim. Preventative measures such as safeguarding personal information, monitoring financial accounts regularly, and promptly reporting suspicious activity are essential in combating identity theft.

How do the bad actors get my information?

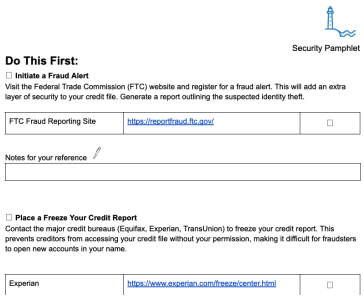
Security breaches of major corporations like Equifax, AT&T, and Verizon can significantly contribute to increased identity theft due to the vast amount of sensitive personal information they hold and pose a significant threat to individuals' personal information and can lead to increased incidents of identity theft. If you suspect that you have become a victim of identity theft, it's crucial to take immediate action to protect yourself. Here's a detailed procedure to follow:

How to use this information to quickly start the steps to protect yourself?

I have divided the process into three sections, Do this First, Do this Second and Do this Last. As you complete each of the sections, you will take the necessary steps to protect yourself. There are some steps that you can take online and others that require you to mail in your information.

Step 1: **Print this PDF Form** 

Step 2: **Start with the First Section “Do this First”**



Security Pamphlet

Do This First:

☐ **Initiate a Fraud Alert**

Visit the Federal Trade Commission (FTC) website and register for a fraud alert. This will add an extra layer of security to your credit file. Generate a report outlining the suspected identity theft.

FTC Fraud Reporting Site	https://reportfraud.ftc.gov/	☐

Notes for your reference

☐ **Place a Freaze Your Credit Report**

Contact the major credit bureaus (Equifax, Experian, TransUnion) to freeze your credit report. This prevents creditors from accessing your credit file without your permission, making it difficult for fraudsters to open new accounts in your name.

Experian	https://www.experian.com/freeze/center.html	☐

Step 3: **Continue to work through the form, use the check boxes ☐ to track your progress.**

Do This First:

☐ **Initiate a Fraud Alert**

Visit the Federal Trade Commission (FTC) website and register for a fraud alert. This will add an extra layer of security to your credit file. Generate a report outlining the suspected identity theft.

FTC Fraud Reporting Site	https://reportfraud.ftc.gov/	☐

Notes for your reference 

☐ **Place a Freeze Your Credit Report**

Contact the major credit bureaus (Equifax, Experian, TransUnion) to freeze your credit report. This prevents creditors from accessing your credit file without your permission, making it difficult for fraudsters to open new accounts in your name.

Experian	https://www.experian.com/freeze/center.html	☐
Equifax	https://www.equifax.com/personal/credit-report-services/credit-freeze/	☐
TransUnion	https://www.transunion.com/credit-freeze	☐
ChexSystems	https://www.chexsystems.com/security-freeze/place-freeze	☐

☐ **Contact Financial Institutions**

Reach out to any institutions that have sent you statements or contacted you for collections regarding unfamiliar accounts. Inform them about the suspected identity theft and request to be connected to their fraud department.

Notes for your reference 

Do This Second:

☐ **File a Police Report**

Visit your local law enforcement authority to file a formal police report regarding the identity theft. Provide as much evidence and documentation as possible to support your case. Bring the original documents you may have received from institutions.

Notes for your reference 

☐ **Mail Extended Fraud Alerts**

Send a written request to the three major credit bureaus (Equifax, Experian, TransUnion) and the banking bureau (ChexSystems) to place a seven-year extended fraud alert on your credit file. This further notifies potential creditors to verify your identity before extending credit.

Experian	No Official Form. Use this template -	☐
Equifax	https://assets.equifax.com/assets/personal/Fraud_Alert_Request_Form.pdf	☐
TransUnion	No Official Form, use general form -	☐
ChexSystems	https://www.chexsystems.com/-/media/Project/ChexSystems/ChexSystems/PDF/Affidavit.pdf	☐

ADDRRESS To Mail Your Applications

Experian	Experian PO Box 9554 Allen, TX 75013	☐
Equifax	Equifax Information Services LLC P.O. Box 105069 Atlanta, GA 30348-5069	☐
TransUnion	TransUnion P.O. Box 2000 Chester, PA 19016	☐
ChexSystems	Chex Systems, Inc. Attn: Consumer Relations PO Box 583399 Minneapolis, MN 55458	☐

Do This Last:

☐ **Secure Personal Accounts**

Change the passwords for your personal email and banking accounts immediately. Use strong, unique passwords and consider enabling two-factor authentication for added security.

☐ **Enable Alerts**

Activate fraud alerts or credit usage alerts on your credit card and banking accounts. This notifies you of any suspicious activity in real-time, allowing you to respond promptly.

☐ **Sign Up for Credit Monitoring**

Consider signing up for a credit monitoring service to keep track of any changes to your credit report. There are free options available, or you can opt for a paid service for additional features.

☐ **Opt-Out of Direct Marketing**

Remove your contact information (phone number, email address, mailing address) from public databases and marketing lists to minimize the risk of further identity theft. Utilize resources such as the FTC's guide on stopping unsolicited mail, phone calls, and emails, as well as opt-out services like Valpak, RedPlum, and Yellow Pages.

Valpak	https://www.valpak.com/remove-address	☐
RedPlum	https://www.save.com/mailing/delivery-options	☐
DMA Choice	https://dmachoice.org/	☐
YellowPages	https://www.yellowpagesoptout.com/	☐

☐ **Notify your employer**

Inform your employer about the identity theft. This is especially important if your work-related information has been compromised or if there is a risk of fraudulent activity affecting your employment status.

☐ **Sign up for Informed Delivery at USPS**

Informed Delivery from USPS can be a valuable tool in helping to detect and prevent identity theft by providing individuals with insights into their incoming mail.

https://reg.usps.com/informeddelivery/welcome

The End. If you have any questions regarding this form, please contact questions@SecurityPamphlet.com