WHAT TO DO IF YOUR PERSONAL INFORMATION IS COMPROMISED

While synthetic identity fraud is not a complete takeover of one's identity, critical pieces of your personal information can be used in creating a synthetic, such as your Social Security number (SSN). The use of your SSN with another identity can alter your credit score, and it may take time for you to discover this activity. Related to synthetic identity fraud is conventional identity theft, in which someone takes over your existing identity, posing as you, and typically either applies for credit or uses your existing accounts. Both scenarios can have devastating effects on your ability to secure additional credit.

HOW DO YOU KNOW IF YOUR INFORMATION HAS BEEN COMPROMISED?

In some cases, you may be contacted directly (e.g., by a company you do business with following a data breach), but in other cases, you may see unusual activity related to your accounts, only to discover that your information has gotten into the wrong hands. The Federal Trade Commission (FTC) offers a list of ***warning signs*** that someone has stolen your personal information.

WHAT SHOULD YOU DO IF YOUR INFORMATION HAS BEEN COMPROMISED?

The FTC also offers the following resources to help individuals whose personal information has been exposed or stolen in some way and then used by another.

DETECTING THE PROBLEM:

A ***checklist of important personal information*** and what to do for each type of information that is lost or exposed.

WHAT TO DO IF YOUR PERSONAL INFORMATION IS COMPROMISED

REPORTING THE PROBLEM:

A ***step-by-step guide*** for reporting when someone is using your personal or financial information to make purchases, get benefits, file taxes or commit fraud.

MOVING FORWARD AND REBUILDING:

A ***personal recovery plan*** that walks you through each step of the recovery process and provides the ability to update and track progress of the personalized plan.

This website offers other resources – such as pre-filled forms, documents and letters – that can be sent to credit reporting agencies, businesses and debt collectors regarding the stolen information. For more information on resources offered by the FTC, visit ***IdentityTheft.gov***.

The synthetic identity fraud mitigation toolkit was developed by the Federal Reserve to help educate the industry about synthetic identity fraud and outline potential ways to help detect and mitigate this fraud type. Insights for this toolkit were provided through interviews with industry experts, publicly available research, and team member expertise. This toolkit is not intended to result in any regulatory or reporting requirements, imply any liabilities for fraud loss, or confer any legal status, legal definitions, or legal rights or responsibilities. While use of this toolkit throughout the industry is encouraged, utilization of the toolkit is voluntary at the discretion of each individual entity. Absent written consent, this toolkit may not be used in a manner that suggests the Federal Reserve endorses a third-party product or service.