Identity Theft
Prevention and Recovery

1. Identity thieves steal private information about another person and then use that information as a disguise to pretend to be that person to officials and on various databases. Your name, birth date, social security number, passwords, and bank and credit card numbers are prime targets for ID thieves. Once the information is stolen, the crook will then attempt one or more of the following categories of attack:

-Attacks on existing credit, such as stealing from your bank account, using your credit card to make unauthorized purchases, or stealing your social security payments or tax refund check;

-Attacks involving new credit, such as obtaining a loan or new credit in your name; or

-Some other, miscellaneous use of your information, such as obtaining a driver's license, a firearm, or classified information.

2. The Federal Trade Commission estimated that nine million people a year are the victims of identity theft, which is probably an understatement. The agency further reported that the dollar volume of identity theft in 2004 alone was over $52 billion. Consumers should protect their personal information, and be constantly vigilant against scams designed to steal cash and information. However the fact of the matter is that even the most sophisticated and cautious among us can not entirely protect against identity theft because we need to rely on others, who are often not very reliable, to protect our information. There are innumerable instances of data breaches of banks, stores, medical facilities, lenders, credit bureaus, schools, health care agencies and others who hold private information. For example,

-For a period of about two months in 2017, hackers had access to data held by Equifax and stole sensitive data of about 143 million Americans;

-In June 2015, sensitive information was stolen from the background investigations held by the Office of Personnel Management of 21.5 million current, former and prospective federal employees;

-On May 3, 2006, the personal laptop and external hard drive of a Veteran's Administration employee were stolen from his home, compromising personal information of 26 million veterans and military personnel.

Unfortunately, these are just some of a long train of incidents resulting in the compromise of personal data.

3. So, knowing that you cannot make your personal information secure, do you just give up? No, you take actions to lessen the risk. Here are some actions that you can take:

-Ensure the physical security of your computers, external hard drives, flash drives, and other data storage equipment on which you have sensitive information;

-Destroy old checks, bank statements and other similar documents by mulching, shredding, or some other means of making them completely unreadable;

--Encrypt sensitive information;

-Use antivirus protection and keep it up to date;

-Delete history, cookies, and temporary Internet cache frequently or set your computer to automatically delete them whenever you exit the internet;

-Use strong passwords to protect your accounts; generally involving upper and lower case letters, wild characters, and numbers;

-Disconnect from the internet when you have completed your browsing session;

-Avoid giving out sensitive information to fraudsters;

-Check your account statements for unauthorized charges;

-Obtain and review your credit report;

-Consider a fraud alert and / or security freeze.

4. Let's take a closer look at those last four items.

a. *Avoid providing information to fraudsters*. It's not as easy as it sounds. Sure, some frauds are easy to spot, such as the email that says you have won the Irish Sweepstakes even though you never entered the contest; or the correspondence from the supposed Nigerian prince imploring you to help him get his millions into the United States. Other scams are more clever: the email pretending to be from your bank or credit card issuer telling you that you need to provide personal information to verify your account; the telephone call from the fake clerk of court asking for your social security number to confirm that you are not the person who violated a jury summons; the call from the fake Red Cross telling you that a loved one has been hurt and then asking for your personal information to confirm you are the proper recipient of such information; the robo-call from the fake IRS telling you that you owe them money and need to contact them right away. Most reputable agencies will not ask for personal information in this

way. In any event, you can find out what, if anything, is really going on by obtaining the company or agency's actual contact information from a reliable source and talking to a representative. Or, better yet, you may be able to call or visit the company or agency personally. Many large companies also post information concerning ongoing scams involving fraudsters pretending to be that company.

b. *Check your account statements for unauthorized charges*. If you know that your credit, ATM, or debit card has been compromised, contact the issuing authority immediately. If you find that there are unauthorized charges on your statement, complain about them immediately to the proper authority. Under federal law, if you make such a complaint soon enough and to the right authority, you can avoid paying these charges. If you were supposed to receive a monthly account statement and didn't, find out why immediately. It is possible that the fraudster had the statement diverted to another address.

c. *Obtain and review your credit report*. How do you know if a crook took out a loan in your name? There's a better way sitting around waiting for debt collection calls for the loan you never initiated, or waiting until a lender declines to give you a loan because of all the adverse entries on your credit report. You can obtain a free annual credit report from each of the three major credit reporting agencies. In fact, you can get a free credit report every four months by rotating among the three major credit reporting agencies. In this way, you can monitor your credit, learn of any inaccurate entries, and dispute them. There are many sites offering credit reports; most of them are commercial sites that want to sell you some credit monitoring service. The official site, ironically not a .gov site, is: https://www.annualcreditreport.com/index.action To make sure you get to the correct site, you may want to go to it by navigating the web page of the Federal Trade Commission, which has a link.

d. *Consider a fraud alert and / or security freeze.*

(1) *Security freeze*. Generally, before anyone will lend you money, they will want to see your credit report. The security freeze prevents anyone from obtaining your credit report unless they have the special password that your create. So, the fraudster has a hard time getting a loan in your name because the lender can't get access to your credit report. If you want to get a loan, you provide the password to the credit reporting agency that unlocks access to your report. Additional information concerning security freeze, sometimes called credit freeze, can be found on the FTC website: https://www.consumer.ftc.gov/articles/0497-credit-freeze-faqs

(2) *Fraud Alert.* If you have been the victim of identity theft or if your personal information has been compromised, you can initiate a fraud alert with the credit reporting agencies. Further, deploying active duty service members can also initiate a fraud alert, whether they have been victimized or not. The fraud alert requires the credit reporting agency to take additional steps to ensure that you want your credit report released. The law does not say what those additional steps are, but it is often a phone call to the number you provide to them. The initial fraud alert lasts 90 days. The FTC web site contains information concerning initial fraud alerts https://www.consumer.ftc.gov/articles/0275-place-fraud-alert as well as extended fraud alerts, which are generally available only you if have created an identity theft report. https://www.consumer.ftc.gov/articles/0279-extended-fraud-alerts-and-credit-freezes

5. **What if someone is already using your personal information to steal from you, obtain loans in your name, or take other adverse actions?** The Federal Trade Commission has an excellent checklist of steps to take to report and recover from identity theft. https://www.identitytheft.gov/ In general, the idea is to take immediate steps to prevent more damage, and then to take steps to repair damage already done. Immediate steps include contacting businesses where you know theft has occurred, obtaining credit reports, initiating a fraud alert, and reporting the theft to the FTC and to local law enforcement. Next, take actions to clean up your credit report and bogus charges on your accounts, initiate an extended fraud alert and consider a security freeze. Certain specialized steps need to be taken to recover from certain types of incidents; e.g. intercept of tax refund, criminal records, use of stolen information to obtain medical services or drugs, etc.

Revised 6 September 2018