STEPS TO TAKE WHEN YOUR IDENTITY HAS BEEN COMPROMISED

#1 - Notify your bank that you are a victim of Identity Theft.

a) - Have the bank issue you a new Debit Card.

b) - Verify that all your checks are intact, then look on your statement for any "out of sequence" checks which may have been cashed.

#2 - Notify ALL your credit card companies that you are a victim of Identity Theft.

a) - Have them issue you new Credit Cards.

#3 - Call the FTC at 1 (877) 438-4338. It IS important that you also go online to the FTC website https://www.identitytheft.gov and fill out (and save a copy) of the "ID theft complaint and affidavit form".

#4 - Contact the police and make a police report about the fact the you are a victim of Identity Theft. You will need the Case Number when you file your Fraud Alert. If they seem reluctant to make a report, provide them with the FTC cover letter from:
https://www.consumer.ftc.gov/sites/default/files/articles/pdf/pdf-0088-ftc-memo-law-enforcement.pdf

Make sure the police report lists all fraud accounts. Give as much documented information as possible and give them a copy of the ID theft complaint form from the FTC. If the police cannot give you a copy of their report, request that they sign your FTC complaint form and provide the police report number in the “Law Enforcement Report” section. Keep the phone number of your police investigator handy on a contact sheet for future reference.

#5 - Contact any one of the 3 credit reporting agencies (Equifax, Experian, or TransUnion), and ask them to add a Fraud Alert. You WILL need to provide them with the police Case Number.

a) - Consider placing a Credit Report freeze (usually free if you provide the police Case Number).

#6 - Request a Credit Report from the credit reporting agency you contacted (it should be provided free). Examine it for any fraudulent activity, such as new accounts you didn’t open, hard inquiries you don’t recognize, payment history you can’t account for, an employer you never worked for, and personal information unfamiliar to you. Check the reports again annually (Federal law gives you the right to get a free copy of your credit report every 12 months from each of the three credit bureaus).

#7 - Notify ALL creditors in writing that you are a victim of Identity Theft and include a copy of your ID theft report. Further, ask each affected creditor to provide you and your investigating law enforcement agency with copies of the documents showing fraudulent transactions.

a) Notify Loan companies you are currently doing business with.

b) Notify Telephone and Utility companies you are currently doing business with.

#9 - Change ALL online (and call-in) Passwords/PINs for EVERY account you had to get a login password for (this includes Banks, Utilities, and even you cellphones personal voicemail mailbox PIN). Check in the book you record your numbers/addresses/signups for any older signups you may have forgotten about (amazon, ebay, walmart, etc.).

#10 - Contact the Social Security fraud hot line. Notify the Office of the "Inspector General" if your Social Security number has been fraudulently used. Ask for a copy of your "Personal Earnings and Benefits Statement and check for accuracy".

#11 - Get a new driver’s license from the DMV. Consider replacing any other licenses as well.

MEMO FROM FTC TO LAW ENFORCEMENT

To: Law Enforcement Officer

From: Division of Privacy and Identity Protection
The Federal Trade Commission

Re: **Importance of Identity Theft Report**

The purpose of this memorandum is to explain what an "Identity Theft Report" is, and its importance to identity theft victims in helping them to recover. A police report that contains specific details of an identity theft is considered an "Identity Theft Report" under section 605B of the Fair Credit Reporting Act (FCRA), and it entitles an identity theft victim to certain important protections that can help him or her recover more quickly from identity theft.

Specifically, under sections 605B, 615(f) and 623(a)(6) of the FCRA, an Identity Theft Report can be used to permanently block fraudulent information that results from identity theft, such as accounts or addresses, from appearing on a victim's credit report. It will also make sure these debts do not reappear on the credit reports. Identity Theft Reports can prevent a company from continuing to collect debts that result from identity theft, or selling them to others for collection. An Identity Theft Report is also needed to allow an identity theft victim to place an extended fraud alert on his or her credit report.

In order for a police report to be incorporated in an Identity Theft Report, and therefore entitle an identity theft victim to the protections discussed above, the police report must contain details about the accounts and inaccurate information that resulted from the identity theft. We advise victims to bring a printed copy of their ID Theft Complaint filed with the FTC with them to the police station in order to better assist you in creating a detailed police report so that these victims can access the important protections available to them if they have an Identity Theft Report. The victim should sign the ID Theft Complaint in your presence. If possible, you should attach or incorporate the ID Theft Complaint into the police report, and sign the "Law Enforcement Report Information" section of the FTC's ID Theft Complaint. In addition, please provide the identity theft victim with a copy of the Identity Theft Report (the police report with the victim's ID Theft Complaint attached or incorporated) to permit the victim to dispute the fraudulent accounts and debts created by the identity thief.

For additional information on Identity Theft Reports or identity theft, please visit www.ftc.gov/idtheft.