Recommended steps to follow when addressing issues of identity theft:

1. Contact the local police precinct to file a report.

2. Contact the U.S. Federal Trade Commission (FTC) to file a complaint at (877) 382-4357) or visit www.ftc.gov and click "Consumer Protection," followed by "Consumer Information." This FTC web page has many helpful identity theft topics, including: How to detect it; What to do if your ATM, debit card, or credit card is stolen; and What to do if your identity is stolen, among others.

3. Notify the three (3) major credit bureaus (Equifax, Experian, and TransUnion) to flag your files with fraud alerts, place creditors on notice that you are a victim of identity theft or fraud, and require creditors and lenders to affirmatively verify your identity prior to opening or changing an account in your name.

   An initial fraud alert is free for one year, and may be extended by the credit bureaus for seven years, if the victim provides a police or FTC complaint number. This will also result in removing you from credit card and insurance offers for five years. Additionally, active military personnel can request placement of an active duty alert with the credit bureaus for one year at no charge in an effort to prevent identity theft or fraud while deployed. The New York State Attorney General's Office lists the following fraud help lines to contact these credit bureaus:

   - Equifax (800) 525-6285;
   - Experian (888) 397-3742;
   - TransUnion (800) 680-7289

4. Obtain a free credit report from each of these credit reporting companies when placing the fraud alert on your file. As a victim of a fraud you are entitled to one (1) free credit report for an initial fraud alert or two (2) free credit reports for an extended fraud alert from each of the nationwide credit reporting companies during a twelve (12) month period. It is important to review your credit reports to determine if there has been any unauthorized activity and to periodically check your credit reports over the next year to ensure that no new fraudulent or unauthorized activity has occurred. Whether you are a victim of credit card fraud or a stolen identity, you need to check your credit reports for any accounts you may not recognize.

   The free credit reports acquired in connection with an initial or extended fraud alerts are separate from the free annual report to which you are also entitled. While plenty of websites and creditors promise free credit reports, the official site to request them is www.AnnualCreditReport.com.

5. Contact banks and credit card companies where you maintain accounts to request a fraud alert and/or to advise said financial companies of the breach of personal information.

6. Review current and older credit card and bank statements for other unauthorized charges you don't recognize. Identity thieves may start with charges or withdrawals as small as $1 to test the waters. Don't forget to review dormant or infrequently used accounts as well. If you find unknown charges, call the financial institution to alert them of the problem and request that the account be locked or closed.

7. Be Alert to "Phishing". A phishing or email-based attack is a fraudulent attempt to obtain sensitive information such as usernames, passwords, and credit card details by disguising oneself as a trustworthy entity. Phishing attacks fall into 4 categories: emails that impersonate a brand, emails that impersonate a trusted individual; emails that mimic a well-known domain; and emails from accounts that have been compromised (i.e., a cybercriminal has hacked into your friend's email account).

   The best form of defense against phishing is to be alert and never give out sensitive information unless you can be sure you trust to whom you are giving the information.

8. Reset and Use a Strong Password. There is a good reason websites often make you create a strong password when you sign up. That is because one of the ways cybercriminals hack into people's accounts is by trying common number-letter combinations. The longer your password and the more numbers, letters, and symbols it contains, the harder it is for your accounts to be hacked. For the same reason, it is a good idea to regularly change your password.

9. Consider adding comprehensive antivirus protection to secure your cell phone, PC and other devices. Additionally, it is important to comply with updates on your phone, laptop and PC to avoid data breaches by hackers who capitalize on outdated systems. Smartphone antivirus apps are also available to protect your phone from malware. It is also recommended that your cell phone remain locked to avoid unwanted access.

10. Consider purchasing a good ID theft protection service that can help when your identity is compromised. The best providers monitor your credit card transactions and credit score and scour social media and the dark web for evidence your ID has been stolen or misused. In terms of recourse, these services offer reimbursement (usually up to $1 million), coverage for lawyers and experts, and identity restoration specialists to help put everything back together.

11. In recent months, our office has received numerous calls concerning Unemployment Insurance (UI) fraud, in which unknown individuals utilize personal information (perhaps gained from a data breach) to file fraudulent unemployment claims. The FBI is actively investigating complaints, which are not limited to New York State see: https://www.wkbw.com/rebound/fbi-buffalo-investigating-potential-unemployment-benefits-fraud-scheme), and for which the FBI provides the following guidance:
https://www.fbi.gov/news/pressrel/press-releases/fbi-sees-spike-in-fraudulent-unemployment-insurance-claims-filed-using-stolen-identities.

    If you are the victim of UI fraud, it is advised that you immediately report the fraud to the NYS Department of Labor at:
    https://webapps.labor.ny.gov/dews/ui/fraud/report-fraud.shtm.
    The NYS DOL has issued the following in response to UI fraud:
    https://dol.ny.gov/report-fraud together with a 2020 press release, which can be reviewed:
    https://www.dfs.ny.gov/reports_and_publications/press_releases/pr202008131.
    Our office has been notified that the NYS DOL typically responds by notifying the victim that their unemployment benefits will not be impacted by the fraud. Our office further advises UI fraud victims to report the incident to the Federal Trade Commission ((877) 382-4357), to file a police report with the local precinct (it will be in the discretion of the precinct whether a police report will be generated concerning the fraud and ID theft), to request fraud alerts from the three credit bureaus (Equifax, Experian, and Transunion), to inform SSA Fraud Hotline ((800) 269-0271) of the misuse of your Social Security Number, and to secure and review your credit report to ascertain if there has been further unauthorized activity.

We know this sounds like a lot to worry about. However, your legal plan is always here to help. Our helpline for telephone consultations is 1-800-832-5182.