RESPONDING TO IDENTITY THEFT, FRAUD AND CYBERCRIME

Identity Theft and Fraud

Having your identity stolen can be scary and invasive and have damaging effects on your finances, medical records and reputation. If you become a victim, knowing how to respond and report the incident is vital. Here are some tips and resources to help you recover.

In cases of identity theft:

- Make sure you change your passwords for all online accounts. When changing your password, make it a sentence that is 12 or more characters long, and make it unique to that account. You may also need to contact your bank and other financial institutions to freeze your accounts so that the offender is not able to access your financial resources.
- Close any unauthorized or compromised credit or charge accounts. Cancel each credit and charge card. Get new cards with new account numbers. Inform the card companies that someone may be using your identity, and find out if there have been any unauthorized transactions. Close accounts so that future charges are denied. You may also want to write a letter to the company so there is a record of the problem.
- Think about what other personal information may be at risk. You may need to contact other agencies depending on the type of theft. For example, if a thief has access to your Social Security number, contact the Social Security Administration. You should also contact your state's department of motor vehicles if your driver's license or car registration is stolen.
- File a report with your local law enforcement agency. Even if your local police department or sheriff's office doesn't have jurisdiction over the crime (a common occurrence for online crime that may originate in another jurisdiction or even another country), you will need to provide a copy of the law enforcement report to your banks, creditors, other businesses, credit bureaus and debt collectors.
- If your personal information has been stolen through a corporate data breach (when a cyber thief hacks into a large database of accounts to steal information, such as Social Security numbers, home addresses and personal email addresses), you will likely be contacted by the business or agency whose data was compromised with additional instructions as appropriate. You may also contact the organization's IT security officer for more information.
- If stolen money or identity is involved, contact one of the three credit bureaus to report the crime (Equifax at 1-800-525-6285, Experian at 1-888-397-3742 or TransUnion at 1-800-680-7289). Request that the credit bureau place a fraud alert on your credit report to prevent any further fraudulent activity (such as opening an account with your identification) from occurring. As soon as one of the bureaus issues a fraud alert, the other two bureaus are automatically notified.

Additional Resources

- IdentityTheft.gov
    - https://identitytheft.gov/
- Identity Theft Resource Center
    - https://www.idtheftcenter.org/

In cases of Social Security fraud:

If you believe someone is using your Social Security number for employment purposes or to fraudulently receive Social Security benefits, call the Social Security Administration's fraud hotline at 1-800-269-0271. Request a copy of your social security statement to verify its accuracy.

Check out the Social Security Administration's website for additional resources. https://oig.ssa.gov/report-fraud-waste-or-abuse

Find more information at https://www.staysafeonline.org