Karl A. Racine
Attorney General for the District of Columbia

Office of the Attorney General Consumer Alert — Identity Theft

While reviewing your credit card statement, you notice a series of charges that you do not recognize. You later get a collection call from a creditor for a late payment on an account that you never opened. You likely have become the victim of identity theft. Identity theft is a crime in which an imposter obtains your personal information (such as your Social Security number, date of birth, or driver's license number) and uses your identity to do things like open credit accounts in your name, purchase merchandise and services using your credit card, or obtain false credentials, such as an identification card.

Identity theft usually occurs when a thief steals documents from your home, mailbox, garbage, wallet, or steals data from a retailer, health care provider or other company with which you did business. It can also happen when scammers trick consumers into revealing their personal information via the Internet — a practice called "phishing" — or through unsolicited telephone calls. The good news is there are several simple steps you can take if you become the victim of identity theft.

How do I know that I have been a victim of identity theft?

One of the most frequent warning signs that your personal information has been compromised is that you receive a notice that a company where you do business or have an account has experienced a data breach. This means a thief or hacker compromised the company's security and may have stolen some of your personal information. Other warning signs that your personal information may have been stolen by an identity thief include:

- Withdrawals from your bank or other financial account that you didn't make.
- Unfamiliar charges appear on a credit card statement.
- Collections calls for debts you do not owe.
- Bills or financial statements stop arriving in the mail.
- Merchants refuse your checks.
- The IRS notifies you that more than one tax return was filed in your name.

What should I do if I suspect my personal information has been stolen?

1) **File a police report.** In the District of Columbia, the Financial and Cyber Crimes Unit of the Metropolitan Police Department ("MPD") handles identity theft complaints. You should file a complaint with MPD and ask for a police report. MPD can be contacted as follows:

   - Via telephone at 202-727-4159.
   - Via the Internet at https://www.mpdc.dc.gov.
   - In person at your nearest MPD district station.

Connect with the Office of the Attorney General
441 4th Street, NW, Washington, DC 20001
Phone: (202) 727-3400 Fax: (202) 347-8922 TTY: (202) 727-3400
Email: dc.oag@dc.gov
CONSUMER HOTLINE — (202) 442-9828

STAY CONNECTED:

www.oag.dc.gov

2) **Report the theft to your financial institutions.** Immediately call and report the theft to the security or fraud department of each company with which you have an account. Follow up in writing, and include copies (NOT originals) of supporting documents. It's important to notify credit card companies and banks in writing. Send such letters by certified mail, return receipt requested, so you can document what the company received and when. Keep a file of your correspondence and enclosures. If the identity thief has made charges or debits on your accounts, or has fraudulently opened new accounts, ask the company to close the accounts or replace your credit cards. Also ask the company to send you forms to dispute those transactions:

   - For charges and debits on existing accounts, ask the representative to send you the company's fraud dispute forms. Write to the company at the address given for "billing inquiries," NOT the address for sending your payments.
   - For new unauthorized accounts, ask if the company has specific fraud dispute forms. If the company already has reported these accounts or debts on your credit report, dispute this fraudulent information by calling the national credit reporting agencies (see below).

3) **Review your credit report.** You should check your credit report regularly for any unusual entries, such as inquiries from companies you haven't contacted, accounts you didn't open, and debts in your name that you don't recognize. You are entitled to one free copy of your credit report every year from each of the national credit reporting bureaus. You are also entitled to a free credit report if you either place a fraud alert or security freeze on your credit report (see below). You can obtain a free copy of your credit report either by calling one of the three national credit reporting agencies or by visiting https://www.annualcreditreport.com. You can contact the three national credit reporting agencies by phone, mail or online:

4) **Place fraud alerts or security freezes on your accounts.** Most businesses will not open a new credit account without first checking your credit report. You can place either a fraud alert or security freeze on your credit report. This alerts businesses who check your credit report that you have been an identity theft victim before they open an account in your name.

TransUnion	**Experian**	**Equifax**
P.O. Box 6790 Fullerton, CA 92834-6790	P.O. Box 9532 Allen, TX 75013	P.O. Box 740241 Atlanta, GA 30374-0241
(800) 680-7289 transunion.com	(888) 397-3742 experian.com	(800) 525-6285 equifax.com

Fraud Alerts

Fraud alerts can help prevent an identity thief from opening accounts in your name. A fraud alert notifies potential creditors that they should take steps to verify your identity before getting a copy of your credit report. To have a fraud alert placed on your credit report, you can contact the three national credit reporting agencies.

Security Freezes

A security freeze (also known as a credit freeze) restricts access to your credit reports, which makes it more difficult for identity thieves to open new accounts in your name. A security freeze does not prevent a thief from making charges to your existing accounts, so you may want to consider closing bank or credit card accounts that may have been compromised. A credit freeze does not affect your credit score. A credit freeze does not stop you from opening a new account, applying for a job, renting an apartment, or buying insurance. But if you're doing any of these, you'll need to lift the freeze temporarily, either for a specific time or for a specific party, such as a potential employer or landlord.

How do I place a freeze on my credit reports?

Contact each of the three credit reporting agencies (see above) and provide the following:

- Your full name, address, Social Security number, and date of birth. If you have moved in the past 5 years, you will need to supply the addresses where you have lived over the prior 5 years.
- Proof of current address, which could be a current utility bill or phone bill.
- For mailed requests, include a photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.).
- The payment of a $10 fee.
- If you are a victim of identity theft, you should provide a copy of any police report.

How do I lift a freeze?

- Contact the credit reporting agencies listed above.
- You may request a temporary lift of the freeze by mail, phone, or the Internet.
- You must provide proper identification.
- You must provide the unique PIN or password provided when you first requested the freeze.
- The freeze must be lifted no later than three (3) business days after receiving your request.

Who can access my credit report once it has been frozen?

- A creditor who requests your file to open a new account will only get a message or a code indicating that the file is frozen.
- You can access your credit report.
- It can be released to your existing creditors; to insurers licensed in the District; as the result of a court order; and for some government purposes, including collecting child support.

Additional Information

For additional information, visit the Federal Trade Commission's website on identity theft at http://ftc.gov/bcp/edu/microsites/idtheft/ or write Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW, Washington, DC 20580. For an **identity theft recovery plan** you can call the FTC's Identity Theft Hotline, toll-free: 1-877-ID-THEFT (438-4338); TTY: 1-866-653-4261 or visit https://Identity Theft.gov.