Consider a “security freeze” or “fraud alert”.

A **security freeze** makes it harder or impossible for somebody to open an account or borrow money in your name using your information. A freeze prevents creditors from accessing your credit files to review your history, thus preventing any new credit from being opened for you, unless you authorize the credit reporting agencies to allow access. To request a freeze, you must contact each of the credit reporting agencies as their credit freeze procedures differ (see below).

A **fraud alert** notifies creditors to contact you before they open new accounts or change existing ones. You can have the three credit bureaus place a 90-day fraud alert, which can be renewed as often as necessary. A fraud alert does not lock down your credit; while creditors will get an alert message, there is no guarantee they will not issue credit.

Visit Experian.com, Equifax.com, and TransUnion.com to find out how to place a freeze or an alert.

ABOUT DFS

The Department of Financial Services oversees approximately 1,700 insurance companies and nearly 500 banks, check cashers, money transmitters, and other financial institutions operating in New York.

Our mission includes ensuring prudent conduct by providers of financial products and services; ensuring fair, timely, and equitable fulfillment of the financial obligations of such providers; encouraging high standards of honesty, transparency, fair business practices, and public responsibility; eliminating financial fraud, other criminal abuse, and unethical conduct in the industry; and educating and protecting consumers of financial products and services.

GET HELP

For more information or to file a complaint, visit the New York State Department of Financial Services website at www.dfs.ny.gov or contact our Consumer Hotline at (800) 342-3736.

NEW YORK STATE OF OPPORTUNITY. Department of Financial Services

What You Need to Know About...

SECURITY BREACHES

This guide is provided for informational purposes only and does not constitute legal advice.

www.dfs.ny.gov

(800) 342-3736

Information about how to respond if you learn that your personal information may have been exposed in a security breach.

WHAT IS A SECURITY BREACH?

A security breach is unauthorized access to your private information held electronically by a business or government institution or nonprofit organization. That private information can include your Social Security Number, medical records, bank account, or credit card number. Criminals can use this information to commit identity theft by making fraudulent purchases, and entering fraudulent transactions in your name.

Security breaches can occur in different ways, including:

- Loss or theft of electronics, for example a phone, flash drive or laptop, containing sensitive information
- Hacking or malware
- Unintended disclosure
- Inadvertent access
- Raiding discarded computers that have not been properly "wiped"

SECURITY BREACH NOTIFICATION

In New York, businesses or organizations that have experienced a security breach must notify consumers of the breach.

Notification can be by letter, email, telephone, through the media, or by information placed on the business's or organization's website.

WHAT TO DO

If you are notified about a security breach, consider the following information:

Is the notice legitimate? If you receive a security breach notice, take steps to confirm that the notice is legitimate and not a scam. Check online to make sure the notice contains verifiable contact information such as a valid website or customer service phone number that matches information on the company's or organization's official website.

Get the facts. Take the time to read the notice. It should state when the breach occurred, what data was affected, and it should provide a contact number or consumer help line. If you have questions, call the company directly, or search online for the company's official website, which should contain information for victims of the breach. Remember to take — and keep — notes from all conversations with company representatives and keep any written material you have about the security breach for your future reference.

Find out what the breaching entity will be doing to reduce your risk of identity theft. If the company or organization that has suffered a breach offers free credit monitoring (or other services) to assist victims of the breach, consider signing up. Credit monitoring will provide regular reviews of your credit report and pick up signs of identity theft and alert you so you can act early to stop theft of your identity.

Be wary of contact by scammers. It's NOT a good idea to provide information to anybody who calls or emails you claiming to be from the company or organization that has experienced a security breach. Don't respond to emails, or click on any links in an email that looks like it came from the breaching entity. These emails could be fraudulent.

Watch for signs of fraud. Not every security breach results in theft or fraud, but you should be vigilant. Check your credit card billing statements for charges you did not make, and monitor your bank and other financial statements. If you spot something suspicious or unusual, report it to your credit card or financial services company immediately.

Review your credit reports. Whether or not you are a breach victim, check your credit reports regularly. By law, you are entitled to a free annual credit report from each of the three major credit reporting agencies (Experian, Equifax, TransUnion), so request a free report from one of the agencies every four months. Review the report carefully for signs of suspicious activity and check out errors and inconsistencies. Checking your credit report will not affect your credit rating. Request your credit reports from all three agencies at www.annualcreditreport.com, or by calling (877) 322-8228.