NEW YORK STATE OF OPPORTUNITY.

Division of Consumer Protection

A Division of the New York Department of State

CONSUMER·ALERT

Equifax Data Breach

Equifax, a "consumer credit reporting agency" (CCRA) reported its computers were hacked, and the hackers accessed personal, identifying information of 143 million consumers, including over 8.3 million New Yorkers.

CCRAs are companies that keep records about consumers' payment history on loans and credit products. If you have ever opened a credit card or loan, personal, identifying information about you has likely been furnished to one or all of the three major CCRAs—Equifax, Experian and TransUnion. Your information may have been hacked.

You are not considered a victim of identity theft just because your information was hacked. To be a victim of identity theft, your information must have been used illegally by someone else. There are affirmative steps you can take to prevent becoming a victim of identity theft after learning your information was stolen.

The New York Department of State recommends consumers use this guide to take steps to protect their identities.

Background

Equifax was hacked on July 29, 2017. Information accessed by the hackers includes consumers' names, birthdates, Social Security numbers, driver's license numbers, credit card numbers, and "dispute documents" containing personal information. The breach may include any other information or documents you have provided Equifax in the past.

Equifax has established a website and call center for consumers: www.equifaxsecurity2017.com, and 1-866-447-7559. Equifax has stated it is sending direct mail notices to consumers whose credit card numbers or dispute documents with personal identifying information were breached.

Protect Your Identity!

Watch Out for Pretexting Calls, "Phishing" Scams, and Attempts to Profit from the Breach

After a data breach like this, scammers will try to get you to give them your personal information by claiming they are from the impacted company, or are going to provide you with some product or service to help you protect your identity. You should be very wary of anyone who reaches out to you offering such a product or service, or claiming to be from Equifax or a similar company.

- ☐ Do not provide information to anyone who calls you claiming to be from Equifax, Experian, TransUnion or some other entity associated with the data breach.
- ☐ Do not provide information in response to an email claiming to be from Equifax, Experian, TransUnion or some other entity associated with the breach.
- ☐ Do not click any email or social media links for products or services claiming to protect your identity, or from an entity seeking your personal information—this includes links to services like "free credit monitoring".
- ☐ Be wary of any individual or entity offering products or services to help you protect your identity, or fix problems related to the Equifax breach.

Consider Taking Action to Protect Yourself

Security Freeze

A "security freeze" or "credit freeze" prevents the CCRAs from sharing your credit report. Your credit report is usually required to open any new consumer credit product, such as a credit card or car loan.

A security freeze will only work if it is placed with all three CCRAs.

To place a security freeze:

☐ Call the dedicated security freeze hotlines, or visit the websites, for each CCRA:

- Experian 888-397-3742, www.experian.com
- Equifax 800-349-9960, www.equifax.com
- TransUnion 888-909-8872, www.transunion.com

You should not have to pay a fee if this is your first time requesting a security freeze, or if you have been victimized by identity theft. If you previously requested a security freeze and did not pay a fee, then the CCRA can charge you $5 for placing a new security freeze. Consumers should not pay a fee unless it is required. It will cost you $5 to temporarily lift the security freeze.

Placing a security freeze means you cannot open new lines of consumer credit until the freeze is lifted. For example, you will not be able to get a car loan or mortgage while a security freeze is in place.

For more information about a security freeze, visit the New York State Department of State Division of Consumer Protection (Click Here).

Fraud Alert

A fraud alert notifies creditors to contact you before they open new accounts or change existing accounts. A fraud alert is not the same as a security freeze; it does not lock down your credit.

Someone can still obtain credit in your name with a fraud alert in place.

A fraud alert generally lasts for 90 days, although it can be extended.

To place a fraud alert:
☐ Contact the CCRAs by phone or through their websites.

Monitor Your Credit Report, Statements and Disclosures:
☐ Check your credit reports regularly.
☐ Obtain a free credit report from each of the three CCRAs once per year.
☐ Visit www.annualcreditreport.com or call 877-322-8228 to obtain these free reports.
☐ Order a report from a different agency every four months, and check it carefully for accounts you did not open and other questionable activity.
☐ Monitor your credit card, monthly bills, and bank statements on a regular basis.

If you see signs of fraud:
☐ Report them immediately to the affected organization, both by phone and certified mail.
☐ Ask your bank or credit card company to put a security block on your account or preemptively request a new credit or debit card.
☐ Consider closing affected bank accounts and opening new ones.

Be Wary of Tax Identity Theft

You should also consider filing your taxes as soon as you can. Scammers often use social security numbers to file tax returns in your name to steal your tax refund. Respond promptly to any Internal Revenue Service correspondence.
If you believe your identity was stolen and income tax filings submitted to the IRS go to www.irs.gov. for specific response instructions.

Commercial Credit Monitoring

Commercial credit monitoring, which may require fees or subscriptions, usually monitors your credit report on a regular basis. It is supposed to spot signs of identity theft and alert you. It is not always foolproof. While they may alert you that your information is being misused, they do not prevent identity theft from occurring.

If you believe you are a victim of identity theft, you must take action; the service will generally not act for you. Different services monitor different activities (for example, credit limit increases, new accounts open in your name, changes to public records), depending on the product.

Make sure you clearly understand the services you will receive before paying for any credit monitoring.

Read and Understand all Terms and Conditions

Read and understand all terms and conditions before you opt to use any product or service, whether free or paid. The terms and conditions may include language to bind you to legal processes more favorable to the company offering the products and services than to you. The terms and conditions may also outline special steps you must take to properly access the benefits and features of the products and services you are selected to use. Make sure you understand these terms and conditions when agreeing to use products intended to help you protect your identity.

You should also be aware certain products or services advertised as “free,” start out free, but then turn into paid or subscription products. You should not have to provide information about any means of payment when signing up for a free service. If asked to provide payment details, you should be sure you understand the circumstances under which the product or service converts from a “free” product or service to a paid product or service.

More Information

The Department of State Division of Consumer Protection provides general consumer education on identity theft in our brochure, “Consumer Guide to Identity Theft.”

The Division of Consumer Protection Identity Theft Prevention and Mitigation Program remains available to assist concerned New Yorkers Monday through Friday from 8:30am to 4:30pm at 1-800-697-1220.