

COUNTY OF SUFFOLK



STEVEN BELLONE
SUFFOLK COUNTY EXECUTIVE

DENNIS M. COHEN
COUNTY ATTORNEY

DEPARTMENT OF LAW

December 6, 2022

VIA E-MAIL

Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
IDtheft@oag.state.md.us

RE: Security Breach Notification

Dear Sir or Madam:

I write on behalf of the Suffolk County of New York (the "County"), located at 100 Veterans Memorial Highway, Hauppauge, New York 11788, to notify your office of a recent incident that may affect the security of certain personal information relating to approximately thirty-eight (38) Maryland residents. This notice will be supplemented with any new and significant facts learned subsequent to its submission. By providing this notice, the County does not waive any rights or defense regarding the applicability of Maryland law, the applicability of the Maryland data event notification statute, or personal jurisdiction.

Nature of the Incident

On or about September 8, 2022, the County discovered that it was a victim of a criminal cyberattack affecting multiple systems throughout the County's network. The County immediately worked to secure its systems with the assistance of third-party forensic specialists, and commenced an investigation into the nature and scope of the incident. On or about November 30, 2022, the County was provided sufficient forensic information to conclude that Social Security numbers of certain Maryland residents were among those affected. This investigation remains ongoing.

As of now, the personal information of Maryland residents that may have been affected includes name, driver's license numbers, and Social Security number.

Notification to Maryland Residents

Promptly after discovering the incident, the County posted information about the incident, with guidance for identity protection. On November 21, 2022, the County posted an updated notice on its website and provided instructions for activating free identity theft monitoring services through Kroll. That same week, Newsday and the New York Times published information about the incident.

The County plans to begin notifying individuals, including the affected Maryland residents, via written notice in the next several days. This notification will include information about the incident and measures that can be taken to protect themselves. A draft copy of the notification is enclosed with this letter.

Steps Taken

The County is offering all potentially impacted individuals, including Maryland residents, the opportunity to enroll in a complimentary twelve-month three bureau credit monitoring plan. The County has changed and strengthened passwords, implemented multi-factor authentication, and introduced new technical safeguards. As it continues through the investigation, the County will continue to assess its security policies and practices and will take steps, as necessary, to minimize the risk of a similar incident occurring in the future.

LOCATION
H. LEE DENNISON BLDG.
100 VETERANS MEMORIAL HIGHWAY ♦

MAILING ADDRESS
P.O. BOX 6100
HAUPPAUGE, NY 11788-0099 ♦

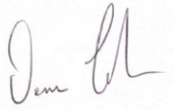
(631) 853-4049
TELECOPIER (631) 853-5169

In addition to providing this notice to your office, the County is providing notice of this incident to other state regulators and the consumer reporting agencies as required.

Contact Information

Should you have any questions regarding this notification or other aspects of this incident, please contact me at (631) 853-5787 or dennis.cohen@suffolkcountyny.gov.

Sincerely,

A handwritten signature in dark ink, appearing to read "Dennis Cohen", is positioned above the printed name.

Dennis Cohen
Suffolk County Attorney

Notice of Data Breach

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>> ,

The Suffolk County government takes your privacy and data security very seriously. The county was the victim of a criminal cyberattack. We are contacting you to explain the incident and provide you with steps you can take to protect yourself. This notification is sent pursuant to the New York State Information and Security Breach and Notification Act (State Technology Law Section 208).

What happened?

On or about September 8, 2022, the County discovered that a cyberattack had apparently occurred on its systems. While the damage assessment continues, it is clear that some personal information was accessed or acquired from the County's systems.

What information was involved?

At this time, we believe that your social security number was among the personal information that may have been accessed and/or acquired.

What we are doing.

We are notifying you so that you can take action to protect yourself. Upon learning of this incident, the County retained cybersecurity firms to conduct a comprehensive investigation into the attack and to ensure that it is fully remediated, to the extent possible. We are also working with experienced legal counsel to help us investigate the data breach and ensure that we are protecting individual safety and following the law. To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, Identity Theft Restoration and Identity Fraud Loss Reimbursement.

Visit <https://enroll.krollmonitoring.com> to activate and take advantage of your identity monitoring services. You have until XXXX to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com. Additional information describing Kroll's services is included with this letter.

<<Date>> (Format: Month Day, Year)
ELN-16037

What you can do.

Please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect yourself, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

We encourage you to regularly review statements from your credit accounts and to remain vigilant in reviewing your credit reports from the three major credit reporting agencies. You may obtain a free copy of your credit report once every 12 months by visiting www.annualcreditreport.com, calling toll-free 877-322-8228 or by completing an Annual Credit Request Form at: www.ftc.gov/bcp/menus/consumer/credit/rights.shtm and mailing it to: Annual Credit Report Request Service P.O. Box 1025281, Atlanta, GA 30348-5283

For more information.

If you have questions about the incident or how to take advantage of Kroll's free services, please call 311 if you are located within Suffolk County or 631-853-6311 if located outside the County Monday through Friday from 9:00 a.m. to 6:00 p.m. Eastern Time or Saturday through Sunday from 9:00 a.m. to 4:00 p.m. Eastern Time.

Protecting your information is important to us. We apologize for any inconvenience this data breach may cause. We hope that the services we are offering to you demonstrate our continued commitment to your security and our appreciation for your dedicated public service.

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228**.

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

The **New York Attorney General** may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; <https://ag.ny.gov/>. The **New York Department of State, Division of Consumer Protection** may be contacted at: <https://dos.nysits.acsiterefactory.com/consumer-protection>



TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

\$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to \$1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit services, you must be over the age of 18 and have established credit in the U.S., have a Social Security number in your name, and have a U.S. residential address associated with your credit file.