



Laura K. Funk, Partner
Cybersecurity & Data Privacy Team
1201 Elm Street, Suite 2550
Dallas, Texas 75270
LFunk@constangy.com
Direct: 248.709.9385

September 7, 2023

VIA EMAIL

Anthony G. Brown
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, Maryland 21202

Email: idtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Brown:

Constangy, Brooks, Smith & Prophete, LLP represents the New York Council of Nonprofits, Inc. ("NYCON") in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland's data breach notification statute.

Nature of the Security Incident

On June 15, 2023, NYCON discovered it was the victim of a sophisticated cybersecurity attack affecting its computer network. Upon discovering this activity, NYCON took immediate steps to secure its network. It also engaged a leading cybersecurity firm to assist with a forensic investigation to determine what happened and evaluate the extent of the unauthorized activity, including what information may have been accessed. After completion of the investigation and a thorough review of potentially affected files, on July 25, 2023, NYCON confirmed that some personal information for employees, contractors and program participants associated with NYCON may have been impacted. NYCON then immediately began collecting up-to-date contact information for those potentially impacted individuals and arranged for notification letters to be sent as soon as possible.

The potentially impacted information of Maryland residents may have included name and Social Security number. NYCON has no evidence of the successful or attempted misuse of any of this information.

Number of Maryland Residents Involved

On August 30, 2023, NYCON notified two (2) Maryland residents of this incident via U.S. First-Class Mail. A sample copy of the notification letter sent to the impacted individuals is included with this correspondence.

Steps Taken to Address the Incident

NYCON has implemented additional security measures in its environment to reduce the risk of a similar incident occurring in the future. In addition, NYCON has provided Maryland residents with complimentary credit monitoring and identity protection services – for a period of 12 months – along with additional resources to assist them. NYCON has also established a toll-free call center to address any questions and to help individuals resolve issues if their identity is compromised due to this incident.

Contact Information

NYCON remains dedicated to protecting the information in its control. If you have any questions or need additional information, please do not hesitate to contact me at LFunk@Constangy.com or 248.709.9385, or David Rice at drice@constangy.com or 718.614.2656.

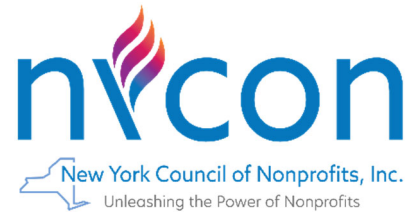
Sincerely,



Laura K. Funk
Partner
CONSTANGY, BROOKS, SMITH & PROPHETE,
LLP

Enclosure: Sample Notification Letter

New York Council of Nonprofits, Inc.
c/o Cyberscout
P.O. Box 3923
Syracuse, NY 13220



To enroll in credit monitoring services, please visit:
<https://secure.identityforce.com/benefit/nycon>
Enrollment Code: FB8VR8D96M

August 30, 2023

Subject: Notice of Data Security Incident

Dear [REDACTED]:

This letter is to inform you of a data security incident experienced by the New York Council of Nonprofits, Inc. ("NYCON") that may have affected your personal information. Please read this letter carefully as it contains important details about the incident and resources you may use to help protect your personal information. NYCON takes this matter extremely seriously as the security of our networks and the information we store is of paramount importance. We apologize for any worry or inconvenience this may cause you.

What Happened? On June 15, 2023, we discovered NYCON had been the victim of a sophisticated cybersecurity attack affecting our computer network. Upon discovering this activity, we took immediate steps to secure our network. We also engaged a leading cybersecurity firm to assist with a forensic investigation to determine what happened and evaluate the extent of the unauthorized activity, including what information may have been accessed. After completion of the investigation and a thorough review of potentially affected files, on July 25, 2023 we confirmed that some personal information for employees, contractors and program participants associated with NYCON may have been impacted. We then immediately began collecting up-to-date contact information for those potentially impacted individuals and arranged for notification letters to be sent as soon as possible.

What Information Was Involved? The potentially affected information may have included your name and Social Security number. Please note that NYCON has no evidence that your information has been misused.

What Are We Doing? As soon as we discovered this incident, we took steps to secure our network and enlisted a leading cybersecurity firm to conduct a forensic investigation, including to figure out how our system was accessed. We have also implemented many additional security measures – and continue to actively seek other steps we can take – to help reduce the risk of a similar incident occurring in the future.

What Should You Do to Protect Your Information? Out of an abundance of caution, we are providing you with access to Single Bureau Credit Monitoring/Single Bureau Credit Report/Single Bureau Credit Score services at no charge. These services provide you with alerts for twenty-four (24) months from the date of enrollment when changes occur to your credit file. This notification is sent to you the same day that the change or update takes place with the bureau. Finally, we are providing you with proactive fraud assistance

to help with any questions that you might have or in event that you become a victim of fraud. These services will be provided by Cyberscout through Identity Force, a TransUnion company specializing in fraud assistance and remediation services.

How Do I Enroll for the Free Services? To enroll in Credit Monitoring¹ services at no charge, please log on to <https://secure.identityforce.com/benefit/nycon> and follow the instructions provided. When prompted please provide the following unique code to receive services: [REDACTED]

What Else Can You Do? In addition to enrolling in the free services above, we recommend that you review the guidance included with this letter about further steps you can take to protect your information.

For More Information: Representatives are available for 90 days from the date of this letter, to assist you with questions regarding this incident, between the hours of 8:00 a.m. to 8:00 p.m. Eastern time, Monday through Friday, excluding holidays. Please call the help line at 1-833-512-0362 and supply the specialist with your unique code listed above.

We take your trust in NYCON and this matter very seriously. Please accept our sincere apologies for any worry or inconvenience that this may cause you.

Sincerely,



Megan T. Allen
Chief Executive Officer
New York Council of Nonprofits, Inc.
272 Broadway
Albany, NY 12204

¹ In order for you to receive the monitoring services described above, you must enroll within 90 days from the date of this letter. The enrollment requires an internet connection and e-mail account and may not be available to minors under the age of 18 years of age. Please note that when signing up for monitoring services, you may be asked to verify personal information for your own protection to confirm your identity.

Additional Steps You Can Take to Protect Your Personal Information

Review Your Account Statements and Notify Law Enforcement of Suspicious Activity: As a precautionary measure, we recommend that you remain vigilant by reviewing your account statements and credit reports closely. If you detect any suspicious activity on an account, you should promptly notify the financial institution or company with which the account is maintained. You also should promptly report any fraudulent activity or any suspected incidence of identity theft to proper law enforcement authorities, your state attorney general, and/or the Federal Trade Commission (FTC).

Request a Copy of Your Credit Report: You may obtain a free copy of your credit report from each of the three major credit reporting agencies once every 12 months by visiting <https://www.annualcreditreport.com>, calling toll-free 1-877-322-8228, or by completing an Annual Credit Report Request Form and mailing it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348. You also can contact one of the following three national credit reporting agencies:

Equifax

P.O. Box 105851
Atlanta, GA 30348
1-800-525-6285
www.equifax.com

Experian

P.O. Box 9532
Allen, TX 75013
1-888-397-3742
www.experian.com

TransUnion

P.O. Box 1000
Chester, PA 19016
1-800-916-8800
www.transunion.com

Place a Fraud Alert: You may want to consider placing a fraud alert on your credit report. An initial fraud alert is free and will stay on your credit file for at least one year. The alert informs creditors of possible fraudulent activity within your report and requests that the creditor contact you prior to establishing any accounts in your name. To place a fraud alert on your credit report, contact any of the three credit reporting agencies identified above. Additional information is available at <https://www.annualcreditreport.com>.

Place a Security Freeze: You have the right to put a security freeze on your credit file for up to one year at no cost. This will prevent new credit from being opened in your name without the use of a PIN number that is issued to you when you initiate the freeze. A security freeze is designed to prevent potential creditors from accessing your credit report without your consent. As a result, using a security freeze may interfere with or delay your ability to obtain credit. You must separately place a security freeze on your credit file with each credit reporting agency. In order to place a security freeze, you may be required to provide the consumer reporting agency with information that identifies you, including your full name, Social Security Number, date of birth, current and previous addresses, a copy of your state-issued identification card, and a recent utility bill, bank statement or insurance statement.

Additional Free Resources: You can obtain information from the consumer reporting agencies, the FTC, or from your respective state Attorney General about fraud alerts, security freezes, and steps you can take toward preventing identity theft. You may report suspected identity theft to local law enforcement, including to the FTC or to the Attorney General in your state.

Federal Trade Commission (FTC)

600 Pennsylvania Ave, NW
Washington, DC 20580
consumer.ftc.gov, and
www.ftc.gov/idtheft
1-877-438-4338

Maryland Attorney General

200 St. Paul Place
Baltimore, MD 21202
oag.state.md.us
1-888-743-0023

New York Attorney General

Bureau of Internet and
Technology Resources
28 Liberty Street
New York, NY 10005
1-212-416-8433

North Carolina Attorney General

9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

Rhode Island Attorney General

150 South Main Street
Providence, RI 02903
<http://www.riag.ri.gov>
1-401-274-4400

Washington D.C. Attorney General

441 4th Street, NW
Washington, DC 20001
oag.dc.gov
1-202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA): These rights include to know what is in your file; to dispute incomplete or inaccurate information; to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information; as well as other rights. For more information about the FCRA and your rights pursuant to the FCRA, please visit <https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf>.