



Lindsay Nickle
1201 Elm Street, Suite 2550
Dallas, Texas 75270
lnickle@constangy.com
Direct: 806.535.0274

May 2, 2023

VIA ELECTRONIC SUBMISSION

Attorney General Brian E. Frosh
Office of the Attorney General
St. Paul Plaza
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Fax: (410) 576-6566

Re: Notice of Data Security Incident

To Whom It May Concern:

Constangy, Brooks, Smith & Prophete LLP ("Constangy") represents Business Outreach Center Network ("BOC Net"), a corporation based in Brooklyn, New York, in conjunction with the recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with the Maryland data breach notification statute.

1. Nature of the Security Incident

On February 4, 2023, BOC Net discovered unusual network activity that disrupted access to certain systems. Upon discovering this activity, BOC Net immediately took steps to secure its network and launched an investigation with the assistance of independent cybersecurity experts to determine what happened and whether sensitive information may have been affected. As a result of this investigation, BOC Net learned certain personal information may have been accessed or acquired without authorization during the incident. On or about April 7, 2023, BOC Net completed a comprehensive review of the impacted data potentially containing personal information through which BOC Net identified certain personal information as potentially involved. BOC Net then worked diligently to identify current contact information to issue notification to relevant individuals.

2. Type of Information and Number of Maryland Residents Notified

The data sets potentially accessible by the malicious actor(s) responsible for this incident included an individual's name, and Social Security number. On May 2, BOC Net notified one Maryland resident of this data security incident via U.S. First-Class Mail. A sample copy of the notification letter sent to potentially impacted individuals is included with this correspondence.

3. Steps Taken Relating to the Incident

BOC Net reported this incident to law enforcement and will cooperate as necessary. It has also implemented additional security measures in an effort to prevent a similar incident from occurring in the future. Further, as referenced in the sample consumer notification letter, BOC Net has offered notified individuals 12 months of complimentary services through Kroll, which include credit monitoring, dark web monitoring, a \$1 million identity fraud loss reimbursement policy, and fully-managed identity theft recovery services.

4. Contact Information

BOC Net remains dedicated to protecting the personal information in its possession. If you have any questions or need additional information, please do not hesitate to contact me at lnickle@constangy.com.

Best regards,
/s/ Lindsay Nickle

Very truly yours,

Lindsay Nickle of
CONSTANGY, BROOKS, SMITH & PROPHETE, LLP

Encl: Sample Adult Consumer Notification Letter



<<Date>> (Format: Month Day, Year)

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_2(Subject: Notice of Data [variable text])>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

Business Outreach Center Network (“BOC Net”) is writing to inform you of a recent data security incident that may have involved your personal information. BOC Net takes the privacy and security of all information within its possession very seriously. We are writing to notify you about the incident, provide you with information about steps you can take to help protect your personal information, and offer you the opportunity to activate the complimentary identity monitoring services that BOC Net is making available to you.

What Happened? On February 4, 2023, BOC Net discovered unusual network activity that disrupted access to certain systems. Upon discovering this activity, BOC Net immediately took steps to secure our network and launched an investigation with the assistance of independent cybersecurity experts to determine what happened and whether sensitive information may have been affected. The investigation subsequently revealed that certain personal information may have been accessed or acquired without authorization during the incident. On or about April 7, 2023, we completed a comprehensive review of the impacted data potentially containing personal information which identified your information as potentially involved. We then took steps to notify you of the incident as quickly as possible. <<b2b_text_3(variable text.)>>

What Information Was Involved? The information that may have been impacted includes your name and <<b2b_text_1(data elements)>>.

What Are We Doing? As soon as we discovered this incident, we took the steps described above. In addition, we reported this incident to law enforcement and will cooperate as necessary. We also implemented additional security measures to help reduce the risk of a similar incident occurring in the future. We are further notifying you of this event and advising you about steps you can take to help protect your information.

In addition, out of an abundance of caution, we are offering you complimentary credit monitoring and identity theft protection services through Kroll, a national leader in identity theft protection. These services include 12 months of Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

What Can You Do?

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

You have until <<b2b_text_6(activation deadline)>> 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. Additionally, information describing your services is included with this letter.

For More Information: If you have any questions about this letter, please call [TFN](tel:18008758777), Monday through Friday from 8:00 am to 5:30 pm Central Time, excluding some major U.S. holidays.

Again, at this time, there is no evidence that your information has been misused as a result of this incident. However, we encourage you to take full advantage of this service offering. The security of personal information is our top priority at BOC Net, and we are committed to safeguarding your data and privacy. Please accept our sincere apologies and know that we deeply regret any concern or inconvenience that this may cause you.

Sincerely,

Nancy Carin

Executive Director
BOC Net

Steps You Can Take to HELP Protect Your 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).

Copy of 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 <http://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

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 <http://www.annualcreditreport.com>.

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

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>.



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.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to help 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.