

June 29, 2022

VIA EMAIL

Attorney General Brian Frosh
Maryland Attorney General's Office
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
E-Mail: ldtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Frosh,

Lewis Brisbois Bisgaard & Smith ("Lewis Brisbois") represents Community of Hope D.C. ("COHDC") in connection with a recent data security incident described in greater detail below. COHDC is a non-profit that provides healthcare and housing services to low-income individuals in the Washington D.C. metro area. The purpose of this letter is to notify you of the incident pursuant to Maryland Code, Com. § 14-3504(h).

A brief description of the nature of the security incident:

On February 7, 2022, COHDC learned of a data security incident involving unauthorized access to an email account of one COHDC employee. The incident was discovered when the account's authorized user identified spam messages being sent from the account. In response, COHDC immediately took steps to secure its environment and began to investigate. COHDC also engaged leading, independent cybersecurity experts to help determine what happened and whether personal information had been accessed or acquired without authorization. As a result, COHDC learned that an unauthorized actor may have accessed certain files and data contained within a single Outlook 365 email account between January 27 and February 7, 2022.

COHDC retained a third-party vendor to conduct a manual review of all data contained within the account to identify any sensitive information which was completed on May 9, 2022. COHDC then worked to identify contact information for impacted residents. Through that process, COHDC discovered the account contained PII from 53 Maryland residents.

The number of Maryland residents being notified:

On June 30, 2022, COHDC mailed notification letters to 53 Maryland residents via first class U.S. Mail. A sample copy of the notification letter is attached.

What information has been compromised:

The information varied for each individual but may have included Social Security numbers, driver's license numbers, financial information, health insurance information, and health diagnostic information.

Steps Taken Relating to the incident

As referenced above, COHDC worked with the digital forensics firm to mitigate the risk to data that may have been affected during the incident. It also implemented additional measures to reduce the risk of a similar incident occurring in the future.

As referenced in the notification letter, COHDC is providing residents with information about steps they can take to help protect their personal information. COHDC is also offering residents whose Social Security numbers were involved in the incident one year of complimentary credit and identity monitoring services through IDX.

COHDC remains dedicated to protecting the personal information in its control. If you have any questions or need additional information, please do not hesitate to contact the undersigned at (412) 567-5113 or David Young at (720) 548-3951.

Sincerely,

Lauren D. Godfrey

Lauren D. Godfrey
Lewis Brisbois Bisgaard & Smith, LLP

Enclosure: Sample Notification Letter



10300 SW Greenburg Rd.
Suite 570
Portland, OR 97223



4 Atlantic Street, SW
Washington, DC 20032
www.communityofhopedc.org
202.407.7747

<<First Name>> <<Last Name>>
<<Address1>> <<Address2>>
<<City>>, <<State>> <<Zip>>

To Enroll, Please Call:
1-800-939-4170
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<XXXXXXXXXX>>

June 30, 2022

Subject: Notice of Data Security Incident

Dear <<First Name>> <<Last Name>>:

At Community of Hope D.C. ("COH"), we are committed to protecting the confidentiality and security of the information we receive and maintain. We are writing to inform you of a recent data security incident that may have impacted some of your personal information. While we are unaware of any misuse of your information, we are writing to notify you of the incident, offer you complimentary credit monitoring and identity protection services, and inform you about steps that you can take to help protect your personal information.

What Happened: On February 7, 2022, we learned of a data security incident involving unauthorized access to an email account of one COH employee. In response, we immediately took steps to secure our environment and began to investigate. We also engaged leading, independent cybersecurity experts to help us determine what happened and whether personal information had been accessed or acquired without authorization. As a result, we learned that an unauthorized actor may have accessed certain files and data contained within the account between January 27 and February 7, 2022. We then conducted a thorough review of the impacted information. On May 9, 2022, we learned that your personal information was contained in the email account. We then immediately identified your mailing address and took steps to notify you of this incident.

What Information Was Involved: The information contained in the account may have included your name and <<Variable Data 2>>.

What We Are Doing: To help prevent something like this from happening again, we are implementing additional technical security measures and increasing employee cybersecurity training. We have also notified the FBI of the incident. While we have no indication that your information has been misused, we are nonetheless providing you with information about steps that you can take to help protect your personal information. As a further precaution, we are also offering you 24 months of complimentary credit monitoring and identity protection services through IDX, a data breach and recovery services expert. These services will help to detect possible misuse of your information and will provide you with identity protection support.

What You Can Do: You can enroll in IDX's complimentary credit monitoring and identity protection services by going to <https://app.idx.us/account-creation/protect> or calling 1-800-939-4170. When prompted, please provide the unique code provided above to enroll in the services. The deadline to enroll is September 30, 2022. For more information on how you can protect your personal information, please review the resources provided on the following pages.

For More Information: If you have any questions regarding the incident, please call **1-800-939-4170** between 9 am – 9 pm Eastern Time, Monday through Friday.

The security of your information is a top priority for COH. We take your trust in us and this matter very seriously and we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Leah Garrett
Vice President, Development and Communications

Derek Sykes
Vice President, Finance and Operations

STEPS YOU CAN TAKE TO FURTHER 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).

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

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.

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

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

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>.