BakerHostetler

Baker&Hostetler LLP
2929 Arch Street
Cira Centre, 12th Floor
Philadelphia, PA 19104-2891
T 215.568.3100
F 215.568.3439
www.bakerlaw.com
Daniel A. Pepper
direct dial: 215.564.2456
dpepper@bakerlaw.com

December 10, 2020

VIA OVERNIGHT MAIL

Attorney General Gordon MacDonald
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Incident Notification

Dear Attorney General MacDonald:

I am writing to notify you of a data security incident on behalf of my client, Brooklyn Defender Services ("BDS"), a public defender organization that represents individuals unable to afford an attorney.

On September 13, 2020, BDS concluded its investigation into an incident which determined that in an unauthorized person gained access to some of BDS' employees' email accounts. Upon discovery of the incident, BDS immediately secured the accounts, began an investigation and a computer forensic firm was engaged to assist. The investigation determined that the unauthorized person was able to access the email accounts between April 3, 2020 and May 5, 2020. The investigation was unable to determine whether the unauthorized person actually viewed or acquired any emails or attachments in the accounts, but in an abundance of caution, BDS reviewed all of the emails and attachments in the accounts to identify individuals whose information may have been accessible to the unauthorized person. The information in the accounts may have included the name, address and Social Security number of two New Hampshire residents.

Beginning on December 10, 2020, BDS will mail notification letters via U.S. mail to the two New Hampshire residents whose personal information may have been involved in this incident, in accordance with N.H. Rev. Stat. Ann. § 359-C:20.[1] A copy of the notification letter is enclosed. BDS is offering one year of complimentary credit monitoring and identity theft protection

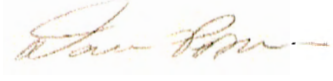
[1] This notice is not, and does not constitute, a waiver of BDS' objection that New Hampshire lacks personal jurisdiction over it regarding any claims related to this data security incident.

services through Kroll to the noticed individual. BDS is also providing a call center for the individuals to call with questions regarding the incident.

To help prevent a similar incident from occurring in the future BDS has incorporated additional authentication measures for remote email access, implemented additional data security measures, and is re-educating its staff for awareness on these types of incidents.

Please do not hesitate to contact me if you have any questions regarding this matter.

Sincerely,



Daniel A. Pepper
Partner

Enclosure

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

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

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

At Brooklyn Defender Services, we recognize the importance of securing and protecting personal information. I am writing to inform you of an incident that involved some of your information. This notice explains the incident, measures we have taken, and some steps you can take in response.

An unauthorized person gained access to some of our employees' email accounts. We immediately secured the accounts, began an investigation, and a computer forensic firm was engaged to assist. The investigation was unable to determine whether the unauthorized person actually viewed or acquired any emails or attachments in the accounts. In an abundance of caution, we reviewed all of the emails and attachments in the account to identify individuals whose information may have been accessible to the unauthorized person and on September 13, 2020 determined that an email or attachment included your <<b2b_text_1 (Impacted Data)>>.

While we have no indication that your information was actually viewed by the unauthorized person, or that it has been misused, we wanted to notify you of this incident and assure you that we take it very seriously. In an abundance of caution, we have arranged for Kroll to provide identity monitoring at no cost to you for one year. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration. For more information on safeguarding your identity, and on Kroll Identity Monitoring, including instructions on how to activate your complimentary one-year membership, please visit the below website:

Visit **https://enroll.idheadquarters.com** to activate and take advantage of your identity monitoring services.

*You have until **March 8, 2021** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

For information on additional steps you can take in response to this incident, please see the additional information provided in this letter.

Your confidence and trust are important to us, and we regret any inconvenience or concern this incident may cause. To further protect personal information, we have added additional authentication measures for remote email access, implemented additional data security measures, and are re-educating our staff for awareness on these types of incidents. If you have any questions, please call 1-???-???-????, Monday through Friday, from 8:00 a.m. to 5:30 p.m. Central Time.

Sincerely,

Lisa Schreibersdorf
Executive Director
Brooklyn Defender Services

Kroll | A Division of DUFF&PHELPS

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

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

Triple Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data at any of the three national credit bureaus—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you will 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 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.

ADDITIONAL STEPS YOU CAN TAKE

We remind you it is always advisable to be vigilant for incidents of fraud or identity theft by reviewing your account statements and free credit reports for any unauthorized activity. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting companies. To order your annual free credit report, please visit www.annualcreditreport.com or call toll free at 1-877-322-8228. Contact information for the three nationwide credit reporting companies is as follows:

- *Equifax*, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111
- *Experian*, PO Box 2002, Allen, TX 75013, www.experian.com, 1-888-397-3742
- *TransUnion*, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-916-8800

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 state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows:

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

Fraud Alerts and Credit or Security Freezes

Fraud Alerts: There are two types of general 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 one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years.

To place a fraud alert on your credit reports, contact one of the nationwide credit bureaus. A fraud alert is free. The credit bureau you contact must tell the other two, and all three will place an alert on their versions of your report.

For those in the military who want to protect their credit while deployed, an Active Duty Military Fraud Alert lasts for one year and can be renewed for the length of your deployment. The credit bureaus will also take you off their marketing lists for pre-screened credit card offers for two years, unless you ask them not to.

Credit or Security Freezes: You have the right to put a credit freeze, also known as a security freeze, on your credit file, free of charge, which makes it more difficult for identity thieves to open new accounts in your name. That's because most creditors need to see your credit report before they approve a new account. If they can't see your report, they may not extend the credit.

How do I place a freeze on my credit reports? There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

- **Experian Security Freeze**, PO Box 9554, Allen, TX 75013, www.experian.com
- **TransUnion Security Freeze**, PO Box 2000, Chester, PA 19016, www.transunion.com
- **Equifax Security Freeze**, PO Box 105788, Atlanta, GA 30348, www.equifax.com

You'll need to supply your name, address, date of birth, Social Security number and other personal information.

After receiving your freeze request, each credit bureau will provide you with a unique PIN (personal identification number) or password. Keep the PIN or password in a safe place. You will need it if you choose to lift the freeze.

How do I lift a freeze? A freeze remains in place until you ask the credit bureau to temporarily lift it or remove it altogether. If the request is made online or by phone, a credit bureau must lift a freeze within one hour. If the request is made by mail, then the bureau must lift the freeze no later than three business days after getting your request.

If you opt for a temporary lift because you are applying for credit or a job, and you can find out which credit bureau the business will contact for your file, you can save some time by lifting the freeze only at that particular credit bureau. Otherwise, you need to make the request with all three credit bureaus.

Additional information to protect your account information

We also recommend that you review any statements that you receive from your health insurer or healthcare providers. If you see services that you did not receive, please contact the insurer or provider immediately.

We remind you to remain vigilant to the possibility of fraud by reviewing your payment card statements for any unauthorized charges. You should immediately report any unauthorized charges to your card issuer because payment card network rules generally provide that cardholders are not responsible for unauthorized charges reported in a timely manner. The phone number to call is usually on the back of your payment card. Please see the pages that follow this notice for additional steps you may take.

We remind you to remain vigilant to the possibility of fraud by reviewing your financial statement for any unauthorized activity. You should immediately report any unauthorized activity to your financial institution.

You should change your password and security question or answer, as applicable, or take other steps appropriate to protect your online account and all other online accounts that use the same username or email address and password or security question or answer.

We remind you to notify other entities that used the same type of biometric data as an authenticator to no longer rely on that data for authentication purposes.

Additional information for residents of the following states

New York: You may contact and obtain information from these state agencies: *New York Department of State Division of Consumer Protection,* One Commerce Plaza, 99 Washington Ave., Albany, NY 12231-0001, 518-474-8583 / 1-800-697-1220, http://www.dos.ny.gov/consumerprotection; and *New York State Office of the Attorney General,* The Capitol, Albany, NY 12224-0341, 1-800-771-7755, https://ag.ny.gov

North Carolina: You may contact and obtain information from your state attorney general at: *North Carolina Attorney General's Office*, 9001 Mail Service Centre, Raleigh, NC 27699, 1-919-716-6000 / 1-877-566-7226, www.ncdoj.gov

West Virginia: You have the right to ask that nationwide consumer reporting agencies place "fraud alerts" in your file to let potential creditors and others know that you may be a victim of identity theft, as described above. You also have a right to place a security freeze on your credit report, as described above.

A Summary of Your Rights Under the Fair Credit Reporting Act: The federal Fair Credit Reporting Act (FCRA) promotes the accuracy, fairness, and privacy of information in the files of consumer reporting agencies. There are many types of consumer reporting agencies, including credit bureaus and specialty agencies (such as agencies that sell information about check writing histories, medical records, and rental history records). Your major rights under the FCRA are summarized below. For more information, including information about additional rights, go to www.consumerfinance.gov/learnmore or write to: Consumer Financial Protection Bureau, 1700 G Street N.W., Washington, DC 20552.

- You must be told if information in your file has been used against you.
- You have the right to know what is in your file.
- You have the right to ask for a credit score.
- You have the right to dispute incomplete or inaccurate information.
- Consumer reporting agencies must correct or delete inaccurate, incomplete, or unverifiable information.
- Consumer reporting agencies may not report outdated negative information.
- Access to your file is limited.
- You must give your consent for reports to be provided to employers.
- You may limit "prescreened" offers of credit and insurance you get based on information in your credit report.
- You have a right to place a "security freeze" on your credit report, which will prohibit a consumer reporting agency from releasing information in your credit report without your express authorization.
- You may seek damages from violators.
- Identity theft victims and active duty military personnel have additional rights.