

CLARK HILL

Robert A. Stern
T 312.519.0362
Email: rastern@clarkhill.com

Clark Hill
130 East Randolph Street
Suite 3900
Chicago, IL 60601
T 312.985.5900
F 312.985.5999
clarkhill.com

September 14, 2020

Via Online Portal

<https://appengine.egov.com/apps/nics/Maine/AGReportingForm>

Attorney General Aaron Frey
Office of the Attorney General
6 State House Station
Augusta, ME 04333

Dear Attorney General Aaron Frey:

We represent James-Bates-Brannan-Groover, LLP (“JBBG”), a law firm, with respect to a data security incident involving the potential exposure of certain personally identifiable information (“PII”) described in more detail below. JBBG is committed to answering any questions you may have about the data security incident, its response, and steps taken to prevent a similar incident in the future.

1. Nature of security incident.

In April 2020, JBBG detected suspicious activity within its email environment. In response to the suspicious activity, JBBG reset the password of the impacted account and contacted its cyber insurance carrier. JBBG then engaged independent computer forensic experts to investigate its network and systems and determine if there was any unauthorized access to client or employee data. Originally, the access appeared to be limited and financially motivated based on relevant search terms and attempts to fraudulently withdraw funds from JBBG’s accounts. However, the forensic investigators informed JBBG that they found suspicious access to multiple accounts, but were unable to determine what emails and attachments, if any, may have been accessed via the unauthorized individual. Thus, out of an abundance of caution, JBBG engaged a second third-party vendor to conduct a comprehensive review of the relevant email accounts to determine all personal information present in those accounts. Once identified, JBBG had to then determine the entity that provided the personal information, whether any of the individuals were represented by counsel, and procure credit monitoring and identity protection services for each potentially impacted individual. JBBG finalized this process on August 17th, 2020. The personal information stored in the relevant email accounts at the time of unauthorized access included some combination of their name, address, date of birth, Social Security number, and a financial account number.

2. Number of residents affected.

September 14, 2020

Page 2

Two (2) Maine residents may have been affected and were notified of the incident. A notification letter was sent to the potentially affected individuals on September 11, 2020 (a copy of the form notification letter is enclosed).

3. Steps taken or plan to take relating to the incident.

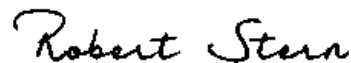
JBBG took steps to address this incident and prevent similar incidents in the future. They contacted law enforcement, changed all passwords, deployed an outlook monitoring software tool, conducted additional anti-virus scanning on all systems, and are currently in the process of implementing multi-factor authentication. Affected individuals were offered 12 months of credit monitoring and identity protection services through ID Experts.

4. Contact information.

JBBG takes the security of the information in its control seriously and is committed to ensuring this information is appropriately protected. If you have any questions or need additional information, please do not hesitate to contact me at rastern@clarkhill.com or (312) 519-0362.

Very truly yours,

CLARK HILL

A handwritten signature in black ink that reads "Robert Stern". The signature is written in a cursive, slightly slanted style.

Robert A. Stern
Attorney

RAS

Enclosure



JAMES BATES
BRANNAN GROOVER LLP
C/O ID Experts
10300 SW Greenburg Rd., Suite 570
Portland, OR 97223

To Enroll, Please Call:

1-800-939-4170

Or Visit:

<https://app.myidcare.com/account-creation/protect>

Enrollment Code: ###

Name
Address 1
Address 2

September 11, 2020

Notice of Data Security Incident

Dear NAME:

James-Bates-Brannan-Groover-LLP (“JBBG”) recently experienced a data security incident that may have impacted your personal or business information. We take the privacy and security of your information seriously, and sincerely apologize for any concern or inconvenience this may cause you. This letter contains information about steps you can take to protect your information and resources we are making available to help you.

1. What happened?

On or around April 16, 2020, JBBG discovered suspicious activity related to a corporate email account. Upon discovering the suspicious activity, we changed all employee passwords and enabled additional security controls to protect the account. We also engaged independent computer forensic experts to conduct a forensic investigation into our email environment. The forensic investigation confirmed that an unauthorized individual gained access to a limited number of corporate email accounts; however, they were unable to identify what emails or attachments, if any, were viewed by the unauthorized individual. Therefore, out of an abundance of caution, JBBG engaged a third party to conduct a comprehensive review of the employees’ mailboxes to determine what personal information may have been present in the accounts.

2. What information was involved?

The mailbox reviews concluded on August 17, 2020, and it appears information provided to these employees via email, including your name, a financial account number and Social Security number was present in the impacted email accounts.

3. What are we doing?

The privacy and security of information entrusted to us is of the utmost importance to us. In response to this incident, we hired an independent third party to investigate and provide recommendations on steps we could take to enhance our existing security protocols. We have since changed all employee passwords, conducted employee training, and are implementing multi-factor authentication on all Office 365 accounts. We are in the process of reviewing our existing information security policies and practices to find other ways we can improve. We are also offering you complimentary credit monitoring services, which are described in more detail below.

4. What can you do?

As a safeguard, we are offering identity theft protection services through ID Experts®, the data breach and recovery services expert, to provide you with MyIDCare™. MyIDCare services include: 24 months of Credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed id theft recovery services. With this protection, MyIDCare will help you resolve issues if your identity happened to be compromised.

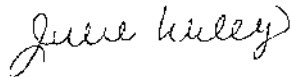
We encourage you to contact ID Experts with any questions and to enroll in free MyIDCare services by calling **1-800-939-4170** or going to <https://app.myidcare.com/account-creation/protect> and using the Enrollment Code provided above. MyIDCare experts are available Monday through Friday from 8 am – 8 pm Central Time. Please note the deadline to enroll is December 11, 2020.

We encourage you to take full advantage of this service offering. Additional information about protecting your identity is included in this letter, 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 also encourage you to review your account statements and explanation of benefits, and to monitor your credit report for suspicious activity.

5. For more information

If you have any questions or concerns, please call **1-800-939-4170** Monday through Friday from 8 am – 8 pm Central Time. Your trust is our top priority, and we deeply regret any inconvenience or concern that this matter may cause you.

Sincerely,

A handwritten signature in cursive script that reads "Julie Wiley".

Julie Wiley, CPA
Chief Operations Officer
James-Bates-Brannan-Groover-LLP

Recommended Steps to Help Protect Your Information

- 1. Website and Enrollment.** Go <https://app.myidcare.com/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code provided at the top of the letter.
- 2. Activate the credit monitoring** provided as part of your MyIDCare membership. The monitoring included in the membership must be activated to be effective. Note: You must have established credit and access to a computer and the internet to use this service. If you need assistance, MyIDCare will be able to assist you.
- 3. Telephone.** Contact MyIDCare at **1-800-939-4170** to gain additional information about this event and speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.
- 4. Review your credit reports.** We recommend that you remain vigilant by reviewing account statements and monitoring credit reports. Under federal law, you also are entitled every 12 months to one free copy of your credit report from each of the three major credit reporting companies. To obtain a free annual credit report, go to www.annualcreditreport.com or call 1-877-322-8228. You may wish to stagger your requests so that you receive a free report by one of the three credit bureaus every four months.

If you discover any suspicious items and have enrolled in MyIDCare, notify them immediately by calling or by logging into the MyIDCare website and filing a request for help.

If you file a request for help or report suspicious activity, you will be contacted by a member of our ID Care team who will help you determine the cause of the suspicious items. In the unlikely event that you fall victim to identity theft as a consequence of this incident, you will be assigned an ID Care Specialist who will work on your behalf to identify, stop and reverse the damage quickly.

You should also know that you have the right to file a police report if you ever experience identity fraud. Please note that in order to file a crime report or incident report with law enforcement for identity theft, you will likely need to provide some kind of proof that you have been a victim. A police report is often required to dispute fraudulent items. You can report suspected incidents of identity theft to local law enforcement or to the Attorney General.

5. Place Fraud Alerts with the three credit bureaus. If you choose to place a fraud alert, we recommend you do this after activating your credit monitoring. You can place a fraud alert at one of the three major credit bureaus by phone and also via Experian's or Equifax's website. A fraud alert tells creditors to follow certain procedures, including contacting you, before they open any new accounts or change your existing accounts. For that reason, placing a fraud alert can protect you, but also may delay you when you seek to obtain credit. The contact information for all three bureaus is as follows:

Credit Bureaus

Equifax Fraud Reporting
1-866-349-5191
P.O. Box 105069
Atlanta, GA 30348-5069
www.equifax.com

Experian Fraud Reporting
1-888-397-3742
P.O. Box 9554
Allen, TX 75013
www.experian.com

TransUnion Fraud Reporting
1-800-680-7289
P.O. Box 2000
Chester, PA 19022-2000
www.transunion.com

It is necessary to contact only ONE of these bureaus and use only ONE of these methods. As soon as one of the three bureaus confirms your fraud alert, the others are notified to place alerts on their records as well. You will receive confirmation letters in the mail and will then be able to order all three credit reports, free of charge, for your review. An initial fraud alert will last for one year.

Please Note: No one is allowed to place a fraud alert on your credit report except you.

6. Security Freeze. By placing a security freeze, someone who fraudulently acquires your personal identifying information will not be able to use that information to open new accounts or borrow money in your name. You will need to contact the three national credit reporting bureaus listed above to place the freeze. Keep in mind that when you place the freeze, you will not be able to borrow money, obtain instant credit, or get a new credit card until you temporarily lift or permanently remove the freeze. There is no cost to freeze or unfreeze your credit files.

7. You can obtain additional information about the steps you can take to avoid identity theft from the following agencies. The Federal Trade Commission also encourages those who discover that their information has been misused to file a complaint with them.

California Residents: Visit the California Office of Privacy Protection (<http://www.ca.gov/Privacy>) for additional information on protection against identity theft.

Kentucky Residents: Office of the Attorney General of Kentucky, 700 Capitol Avenue, Suite 118 Frankfort, Kentucky 40601, www.ag.ky.gov, Telephone: 1-502-696-5300.

Maryland Residents: Office of the Attorney General of Maryland, Consumer Protection Division 200 St. Paul Place Baltimore, MD 21202, www.oag.state.md.us/Consumer, Telephone: 1-888-743-0023.

New Mexico Residents: You have rights pursuant to the Fair Credit Reporting Act, such as the right to be told if information in your credit file has been used against you, the right to know what is in your credit file, the right to ask for your credit score, and the right to dispute incomplete or inaccurate information. Further, pursuant to the Fair Credit Reporting Act, the 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 credit reports to be provided to employers; you may limit “prescreened” offers of credit and insurance you get based on information in your credit report; and you may seek damages from a violator. You may have additional rights under the Fair Credit Reporting Act not summarized here. Identity theft victims and active duty military personnel have specific additional rights pursuant to the Fair Credit Reporting Act. You can review your rights pursuant to the Fair Credit Reporting Act by visiting www.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf, or by writing Consumer Response Center, Room 130-A, Federal Trade Commission, 600 Pennsylvania Ave. N.W., Washington, D.C. 20580.

North Carolina Residents: Office of the Attorney General of North Carolina, 9001 Mail Service Center Raleigh, NC 27699-9001, www.ncdoj.gov, Telephone: 1-919-716-6400.

Oregon Residents: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, www.doj.state.or.us/, Telephone: 877-877-9392

Rhode Island Residents: Office of the Attorney General, 150 South Main Street, Providence, Rhode Island 02903, www.riag.ri.gov, Telephone: 401-274-4400

All US Residents: Identity Theft Clearinghouse, Federal Trade Commission, 600 Pennsylvania Avenue, NW Washington, DC 20580, www.consumer.gov/idtheft, 1-877-IDTHEFT (438-4338), TTY: 1-866-653-4261.