



Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

July 6, 2022

VIA ELECTRONIC SUBMISSION

Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Incident Notification
200 St. Paul Place
Baltimore, MD 21202
Email: ldtheft@oag.state.md.us

Re: Notice of Data Security Incident

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP ("Lewis Brisbois") represents Howard, Kohn, Sprague & Fitzgerald, LLP ("HKSF") in connection with a recent data security incident described in greater detail below.

1. Nature of the security incident.

On March 22, 2022, HKSF identified suspicious activity associated with one employee email account. In response, HKSF took immediate steps to secure the account and promptly launched an investigation. In so doing, HKSF engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result. On May 26, 2022, HKSF learned that personal information belonging to certain individuals associated therewith may have been impacted in connection with the incident. HKSF then took steps to identify current mailing addresses in order to effectuate notification to potentially impacted individuals.

The information that may have been accessible by the malicious actor(s) responsible for this incident includes driver's license numbers.

2. Number of Maryland residents affected.

HKSF notified a single (1) Maryland resident of this incident via first class U.S. mail on July 6, 2022. A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the Incident.

As soon as HKSF discovered this incident, HKSF took steps to secure its email environment and launched an investigation to determine what happened and whether personal information had been

accessed or acquired without authorization. HKSF has also implemented additional safeguards to help ensure the security of its email environment and to reduce the risk of a similar incident occurring in the future.

HKSF has established a toll-free call center through Epiq, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. The call center is available at 1-855-288-5422 from 8:00 A.M. to 8:00 P.M. Central Time, Monday through Friday (excluding holidays). In addition, while HKSF is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, HKSF is also providing complimentary identity protection services to notified individuals.

4. Contact information.

HKSF 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 Lewis Brisbois.

Best regards,



Alyssa R. Watzman
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Sample Notification Letter



Return Mail Processing Center
P.O. Box 6336
Portland, OR 97228-6336

<<MailID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<City>><<State>><<Zip>>
<<Country>>

<<Date>>

Subject: Notice of Data Security Incident

Dear <<Name 1>>,

I am writing to inform you of a recent data security incident experienced by Howard, Kohn, Sprague & Fitzgerald, LLP (“HKSF”) that may have affected your personal information. HKSF takes the privacy and security of all personal information within its possession very seriously. Please read this letter carefully as it contains information regarding the incident and steps that you can take to help protect your information.

What Happened? On March 22, 2022, HKSF identified suspicious activity associated with one employee email account. In response, HKSF took immediate steps to secure the account and promptly launched an investigation. In so doing, HKSF engaged independent digital forensics and incident response experts to determine what happened and to identify any information that may have been accessed or acquired without authorization as a result. On May 26, 2022, HKSF learned that your personal information may have been impacted in connection with the incident which is the reason for this notification. Please note that HKSF has no evidence of the misuse or attempted misuse of any potentially impacted information.

What Information Was Involved? The information potentially impacted in connection with this incident included your name as well as your <<Breached Elements >>.

What Are We Doing? As soon as HKSF discovered this incident, HKSF took the steps described above. In addition, HKSF implemented measures to enhance the security of its email environment in an effort to minimize the risk of a similar incident occurring in the future.

Although HKSF has no evidence of the misuse of any potentially impacted information, HKSF is providing you with information about steps that you can take to help protect your personal information and is offering you a <<CM Length >> months membership to TransUnion Interactive’s myTrueIdentity credit monitoring and identity restoration service at no cost to you. This product provides you with premier credit monitoring and identity theft resolution, including up to \$1 million of identity theft insurance coverage. To receive these services, you must be over the age of 18, 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. The deadline to enroll is <<deadline>>.

What You Can Do: You can follow the recommendations included with this letter to help protect your personal information. HKSF also encourages you to enroll in the complimentary services being offered to you through TransUnion Interactive by using the enrollment code provided below.

For More Information: Further information about how to protect your personal information is included with this letter. If you have questions or need assistance, please contact 877-637-5039, Monday through Friday, 9am – 9pm ET. Our representatives are fully versed on this incident and can answer any questions you may have regarding the protection of your personal information.

Please accept my sincere apologies and know that HKSF takes this matter very seriously and deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

A handwritten signature in blue ink, appearing to read "G. Krieger", followed by a long, sweeping checkmark-like stroke.

Greg S. Krieger, Esq.
Howard, Kohn, Sprague & Fitzgerald, LLP

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>.



Activation Code: <<Activation Code>>

1-Bureau TransUnion Credit Monitoring Product Offering: (Online and Offline)

As a safeguard, we have arranged for you to enroll, at no cost to you, in an online credit monitoring service (*myTrueIdentity*) for <<CM Length>> months provided by TransUnion Interactive, a subsidiary of TransUnion®, one of the three nationwide credit reporting companies.

To enroll in this service, go directly to the *myTrueIdentity* website at www.mytrueidentity.com and in the space referenced as “Enter Activation Code”, enter the following unique 12-letter Activation Code <<Activation Code>> and follow the three steps to receive your credit monitoring service online within minutes.

If you do not have access to the Internet and wish to enroll in a similar offline, paper based, credit monitoring service, via U.S. Mail delivery, please call the TransUnion Fraud Response Services toll-free hotline at **1-855-288-5422**. When prompted, enter the following 6-digit telephone pass code <<Telephone Pass Code >> and follow the steps to enroll in the offline credit monitoring service, add an initial fraud alert to your credit file, or to speak to a TransUnion representative if you believe you may be a victim of identity theft.

Once you are enrolled, you will be able to obtain <<CM Length>> months of unlimited access to your TransUnion credit report and VantageScore® credit score by TransUnion. The daily credit monitoring service will notify you if there are any critical changes to your credit file at TransUnion®, including fraud alerts, new inquiries, new accounts, new public records, late payments, change of address and more. The service also includes the ability to lock and unlock your TransUnion credit report online, access to identity restoration services that provides assistance in the event your identity is compromised to help you restore your identity and up to \$1,000,000 in identity theft insurance with no deductible. (Policy limitations and exclusions may apply.)

You can sign up for the *myTrueIdentity* online Credit Monitoring service anytime between now and <<Enrollment Deadline>>. Due to privacy laws, we cannot register you directly. Please note that credit monitoring services might not be available for individuals who do not have credit file at TransUnion®, or an address in the United States (or its territories) and a valid Social Security number, or are under the age of 18. Enrolling in this service will not affect your credit score.

If you have questions about your *myTrueIdentity* online credit monitoring benefits, need help with your online enrollment, or need help accessing your credit report, or passing identity verification, please contact the *myTrueIdentity* Customer Service Team toll-free at: 1-844-787-4607, Monday-Friday: 8am- 9pm, Saturday-Sunday: 8am-5pm Eastern time.