



LEWIS BRISBOIS BISGAARD & SMITH LLP

Laura K. Funk
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Laura.Funk@lewisbrisbois.com
Direct: 972.942.5696

June 22, 2022

VIA EMAIL

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

Re: Notice of Data Security Incident

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP represents Seigfreid Bingham, PC (“Seigfreid Bingham”) in connection with a data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maryland’s data breach notification statute.

1. Nature of the Security Incident

On October 19, 2021, Seigfreid Bingham learned of a potential security incident involving potentially unauthorized access to its digital environment. Upon discovering this potential unauthorized access, Seigfreid Bingham immediately took steps to further secure its digital environment and began to investigate. It also engaged leading, independent cybersecurity experts to address the potential incident and conduct an investigation. As a result of the investigation, Seigfreid Bingham learned that an unauthorized actor accessed certain files and data stored within its digital environment. After a thorough and extensive review of the potentially impacted data, it determined on May 19, 2022, that the personal information of Maryland residents may have been impacted by this incident. The information accessed without authorization varies by individual, but may have included the residents’ first and last name, driver’s license or state identification number, payment card numbers, payment card access information, and/or Social Security number. To date, Seigfreid Bingham has no evidence that any of this information has been misused.

2. Number of Maryland Residents Affected

On June 22, 2022, Seigfreid Bingham notified two (2) Maryland residents of this data security incident via First-Class U.S. Mail. A sample copy of the notification letter sent to the affected individuals is attached.

3. Steps Taken Relating to the Incident

To help reduce the risk of something like this from happening again, Seigfreid Bingham has implemented additional technical security measures. Additionally, it is providing impacted individuals with information about steps that they can take to help protect their personal information. As a further precaution, Seigfreid Bingham is also offering to those whose Social Security numbers were impacted identity theft protection services through IDX, which includes 12 months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

4. Contact Information

Please feel free to contact me at 972.942.5696 or Laura.Funk@lewisbrisbois.com if you have any further questions.

Sincerely,

A handwritten signature in cursive script that reads "Laura K Funk".

Laura K. Funk of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl: Sample Individual Notification Letter



SEIGFREID
BINGHAM

10300 SW Greenburg Rd. Suite 570
Portland, OR 97223

To Enroll, Please Call:

1-800-939-4170

Or Visit:

[https://app.idx.us/account-
creation/protect](https://app.idx.us/account-creation/protect)

Enrollment Code:

<<XXXXXXXX>>

<<First Name>> <<Last Name>>

<<Address1>> <<Address2>>

<<City>>, <<State>> <<Zip>>

June 22, 2022

Subject: Notice of Data <<Variable 1>>

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

We are writing to inform you about an incident that may have involved your personal information. You may not have heard of our firm - Seigfreid Bingham, PC, in Kansas City, Missouri – but we provide legal services to various entities. We are committed to protecting the confidentiality and security of the information we receive and maintain, and as such are notifying you of an incident, offering you complimentary credit monitoring and identity protection services, and informing you about steps you can take to help protect your personal information.

What Happened: On October 19, 2021, Seigfreid Bingham learned of a potential security incident involving unauthorized access to our digital environment. Upon discovering this potential unauthorized access, we immediately took steps to further secure our digital environment and began to investigate. We also engaged leading, independent cybersecurity experts to help us to address the potential incident and conduct an investigation. As a result of the investigation, we learned that an unauthorized actor accessed certain files and data stored within a portion of our digital environment. After a thorough and extensive review of the potentially impacted data, we learned on May 19, 2022, that your personal information may have been impacted by this incident. Notably, we have no evidence that any personal information potentially impacted by this incident has been misused, but we are nonetheless providing notification out of an abundance of caution.

What Information Was Involved: Seigfreid Bingham completed a detailed, time-intensive review of the data that may have been accessed by the unauthorized actor and determined that information included your name, <<Variable 2>>.

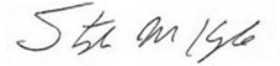
What We Are Doing: To help reduce the risk of something like this from happening again, we have implemented additional technical security measures. Additionally, we are providing you with information about steps that you can take to help protect your personal information. As a further precaution, we are also offering you identity theft protection services through IDX, which includes <<Variable 3>> months of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services. With this protection, IDX will help you resolve issues if your identity is compromised.

What You Can Do: You can enroll in IDX's complimentary credit and identity monitoring services by going to <https://app.idx.us/account-creation/protect> or calling 1-800-939-4170 between 8 a.m. to 8 p.m. Central Time from Monday to Friday. When prompted, please reference the unique code provided above to enroll in the services. The deadline to enroll is September 22, 2022. For more information on how you can protect your personal information, please review the resources provided on the following pages.

For More Information: You will find detailed instructions for enrollment on the enclosed Recommended Steps document. Also, you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter. Please call 1-800-939-4170 between 8 a.m. to 8 p.m. Central Time from Monday to Friday or go to <https://app.idx.us/account-creation/protect> for assistance or for any additional questions you may have.

The security of your information is a top priority for Seigfreid Bingham. 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,

A handwritten signature in dark ink, appearing to read "Steve M Kyle", is positioned above the printed name and title.

Stephen M. Kyle
CEO

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).

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>.