



Aubrey L. Weaver
550 E. Swedesford Road, Suite 270
Wayne, Pennsylvania 19087
Aubrey.Weaver@lewisbrisbois.com
Direct: 215.253.7506

May 24, 2022

VIA ONLINE SUBMISSION

Attorney General Aaron Frey
Maine Attorney General's Office
Consumer Protection Division
6 State House Station
Augusta, ME 04333

Re: Notice of Data Security Incident

Dear Attorney General Frey:

We represent Singleton Schreiber, LLP ("Singleton Schreiber"), a law firm based in San Diego, California, in connection with a data security incident described in greater detail below. Singleton Schreiber takes the protection of all information within its possession very seriously and is taking steps to help prevent similar incidents from occurring in the future. We are writing to notify you that this incident may have affected the personal information of five (5) Maine residents.

1. Nature of the Security Incident.

On October 8, 2021, Singleton Schreiber began observing unusual activity within its network environment and discovered that certain network systems had been disrupted. Upon learning of this, Singleton Schreiber immediately took steps to secure its environment and launched an investigation with the assistance of outside cybersecurity experts. Based on the results of the investigation, Singleton Schreiber learned that certain data in its environment may have been accessed or acquired without authorization during the incident. Singleton Schreiber thereafter undertook a comprehensive review of the potentially affected data to identify any individuals whose sensitive information may have been involved and took steps to gather contact information for those individuals, which process concluded on April 13, 2022.

Based on its review, Singleton Schreiber learned that the incident may have involved the Maine residents' names, Social Security numbers, driver's license or state identification card numbers, and/or medical information.

2. Number of Maine Residents Affected.

Singleton Schreiber notified five (5) potentially affected Maine residents via first class U.S. mail on April 29, 2022, via the attached notification letter template, or a substantially similar version thereof.

3. Steps Taken Relating to the Incident.

As soon as Singleton Schreiber discovered this incident, it took steps to secure its systems and launched an investigation to determine what happened and whether personal information had been accessed or acquired without authorization. Singleton Schreiber has also implemented additional safeguards to help ensure the security of its systems and to reduce the risk of a similar incident occurring in the future.

Singleton Schreiber has established a toll-free call center through IDX to answer questions about the incident and address related concerns. In addition, Singleton Schreiber is offering twelve (12) months of complimentary credit and identity monitoring services to all potentially affected individuals.

4. Contact Information.

Singleton Schreiber 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 me at 215.253.7506 or via email at Aubrey.Weaver@lewisbrisbois.com.

Very truly yours,



Aubrey Weaver of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

Encl.: Sample Consumer Notification Letter



Return to: IDX
P.O. Box 989728
West Sacramento, CA 95798-9728

To Enroll, Please Call:
1-833-774-2038
Or Visit:
<https://app.idx.us/account-creation/protect>
Enrollment Code: <<ENROLLMENT>>

<<FIRST NAME>> <<LAST NAME>>
<<ADDRESS1>>
<<ADDRESS2>>
<<CITY>>, <<STATE>> <<ZIP>>
<<Country>>

April 29, 2022

Subject: Notice of <<Variable Text 1>>

Dear <<FIRST NAME>> <<LAST NAME>>:

Singleton Schreiber, LLP (“Singleton Schreiber”) is writing to inform you of a data security incident that may have impacted your personal information. We take the privacy and security of your information very seriously. That is why we are writing to provide additional information about the incident, offer you complimentary identity protection services, and inform you about steps that you can take to help protect your information.

What Happened? On October 8, 2021, we discovered a data security incident impacting certain systems. We immediately launched an investigation and took steps to secure our network. We also engaged an independent digital forensics firm to assist with the investigation and determine what happened and whether sensitive information may have been accessed or acquired during the incident. Through the course of our investigation, we learned that some files were acquired from our network environment between October 3 and 8, 2021. We thereafter launched a comprehensive review of the potentially affected files to identify any sensitive information that may have been contained therein and to gather up-to-date contact information needed to provide notice to all potentially affected individuals, which concluded on April 13, 2022.

What Information Was Involved? The potentially affected information may have included your <<Variable Text 2>>.

What Are We Doing? As soon as we discovered this incident, we took the measures described above. We have also taken measures to improve our systems in an effort to mitigate against the evolving cybersecurity risks that all businesses face and reduce the likelihood of a similar incident occurring in the future. We also reported the incident to the Federal Bureau of Investigation and will provide whatever cooperation is necessary to facilitate prosecution of the perpetrators.

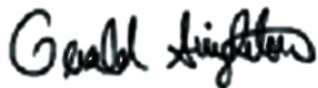
In addition, we are providing you with information about steps that you can take to help protect your personal information and, as an added precaution, we are offering you complimentary identity protection services through IDX, a data breach and recovery services expert. IDX identity protection services include: <<monitoring length>> of credit and CyberScan monitoring, a \$1,000,000 insurance reimbursement policy, and fully managed identity theft recovery services.

What Can You Do? You can follow the recommendations included with this letter to help protect your information. In addition, you can enroll in free identity protection services by calling 1-833-774-2038 or going to <https://app.idx.us/account-creation/protect> and using the Enrollment Code provided above. IDX representatives are available Monday through Friday from 6:00 am to 6:00 pm Pacific Time. Please note the deadline to enroll is July 29, 2022.

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 call 1-833-774-2038 or go to <https://app.idx.us/account-creation/protect>. IDX representatives are fully versed on this incident and can answer any questions you may have regarding this incident and the protection of your personal information.

Singleton Schreiber takes your trust in us and this matter very seriously and deeply regrets any worry or inconvenience that this may cause you.

Sincerely,

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

Gerald Singleton, Esq.
Managing Partner

Singleton Schreiber, LLP
450 A. Street, 5th Floor
San Diego, California 92101

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>.

IDX Identity Protection Services

Website and Enrollment. Please visit <https://app.idx.us/account-creation/protect> and follow the instructions for enrollment using your Enrollment Code included with this letter.

Activate the credit monitoring provided as part of your 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, IDX will be able to assist you.

Telephone. Contact IDX at 1-833-774-2038 to speak with knowledgeable representatives about the appropriate steps to take to protect your credit identity.

IDX Identity will include <<monitoring length>> of enrollment into the following service components:

SINGLE BUREAU CREDIT MONITORING - Monitoring of credit bureau for changes to the member's credit file such as new credit inquires, new accounts opened, delinquent payments, improvements in the member's credit report, bankruptcies, court judgments and tax liens, new addresses, new employers, and other activities that affect the member's credit record.

CYBERSCANTM - Dark Web monitoring of underground websites, chat rooms, and malware, 24/7, to identify trading or selling of personal information like SSNs, bank accounts, email addresses, medical ID numbers, driver's license numbers, passport numbers, credit and debit cards, phone numbers, and other unique identifiers.

IDENTITY THEFT INSURANCE - Identity theft insurance will reimburse members for expenses associated with restoring their identity should they become a victim of identity theft. If a member's identity is compromised, the policy provides coverage for up to \$1,000,000, with no deductible, from an A.M. Best "A-rated" carrier. Coverage is subject to the terms, limits, and/or exclusions of the policy.

FULLY-MANAGED IDENTITY RECOVERY – IDX's fully-managed recovery service provides restoration for identity theft issues such as (but not limited to): account creation, criminal identity theft, medical identity theft, account takeover, rental application, tax fraud, benefits fraud, and utility creation. This service includes a complete triage process for affected individuals who report suspicious activity, a personally assigned ID Care Specialist to fully manage restoration of each case, and expert guidance for those with questions about identity theft and protective measures.