LEWIS BRISBOIS BISGAARD & SMITH LLP

Lauren D. Godfrey
429 Fourth Avenue, Suite 805
Pittsburgh, Pennsylvania 15219
Lauren.Godfrey@lewisbrisbois.com
Direct: 412.567.5113

October 28, 2021

File No. 36629.197

VIA WEB PORTAL

Attorney General Aaron Frey
Office of the Attorney General
Consumer Protection Division
Security Breach Notification
111 Sewall Street, 6th Floor
Augusta, ME 04330

Re: **Notification of Data Security Incident**

Dear Attorney General Frey:

Lewis Brisbois Bisgaard & Smith LLP represents Aronsohn Weiner Salerno & Kaufman, PC (Aronsohn Weiner) in connection with a recent data security incident described in greater detail below. The purpose of this letter is to notify you of the incident in accordance with Maine's data breach notification statute.

1. Nature of the Security Incident

Aronsohn Weiner is a law firm located in New Jersey.

On February 26, 2021, Aronsohn Weiner discovered unusual activity within its Microsoft Office 365 environment. Immediately upon discovery, Aronsohn Weiner took steps to secure its email environment. Additionally, Aronsohn Weiner retained cybersecurity and digital forensics experts as well as incident response counsel to assist with its response efforts and conduct an investigation to determine the source and scope of the incident.

The investigation revealed that an unauthorized actor was able to access three Aronsohn Weiner employees' e-mail accounts. Further, the investigation determined personal information may have been impacted as a result of the incident. Aronsohn Weiner then worked diligently to identify address

information associated with such individuals in order to provide notification of this incident. This process was completed on October 6, 2021.

2. Type of Information and Number of Maine Residents Involved

The incident involved personal information for approximately 1 Maine resident. The information involved differs depending on the individual, but may include Social Security number, Driver's License number, tax information, medical history, condition, treatment, diagnosis, credit card number, and financial account information.

The affected individual will receive a letter notifying them of the incident, offering complimentary identity monitoring services, and providing additional steps they can take to protect their personal information. The notification letters will be sent via USPS First Class Mail on October 28, 2021.

3. Measures Taken to Address the Incident

In response to the incident, Aronsohn Weiner retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise.

As discussed above, Aronsohn Weiner is notifying the affected individuals and providing them with steps they can take to protect their personal information, including enrolling in the complimentary identity monitoring services offered in the notification letter.

4. Contact Information

Aronsohn Weiner is dedicated to protecting the sensitive information within its control. If you have any questions or need additional information regarding this incident, please do not hesitate to contact Lauren Godfrey at Lauren.Godfrey@lewisbrisbois.com.

Sincerely,

Lauren D. Godfrey

Lauren D. Godfrey of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

LDG:vhn

Encl.: Sample Notification Letter

ARONSOHN WEINER SALERNO & KAUFMAN, P.C.

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

To Enroll, Please Call:
866-243-0734
Or Visit:
www.equifax.com/activate
Activation Code: **<<Activation Code>>**

<<Mail ID>>
<<Name 1>>
<<Name 2>>
<<Address 1>>
<<Address 2>>
<<Address 3>>
<<Address 4>>
<<Address 5>>
<<City>><<State>><<Zip>>
<<Country>>

October 28, 2021

Re: Notice of Data Security Incident

Dear <<Name 1>>,

I am writing to inform you of a recent data security incident experienced by Aronsohn Weiner Salerno & Kaufman PC ("Aronsohn Weiner") that may have involved your personal information. At Aronsohn Weiner, we take the privacy and security of all of the information in our possession very seriously. That is why we are writing to notify you of the incident and to provide you with steps that you can take to help protect your personal information.

What Happened. On February 26, 2021, we discovered unusual activity within our Microsoft Office 365 environment. Upon discovery, we took immediate steps to secure the environment. In addition, we retained outside cybersecurity experts to conduct an investigation to determine the source and scope of the incident.

The investigation revealed that an unauthorized actor was able to access three employees' e-mail accounts. Based on the findings from the investigation, we reviewed the affected accounts to determine what data might have been involved. We determined that at least one of the impacted accounts contained some of your personal information. We then worked diligently to identify addresses for the individuals whose information may have been involved, which was completed on October 6, 2021. Importantly, Aronsohn Weiner is not aware of any misuse of your personal information as a result of this incident.

What Information Was Involved. The information may have involved <<data elements>>.

What We Are Doing. As soon as we detected the incident, we took the measures referenced above. We are also providing you information about steps you can take to help protect your personal information and offering free credit monitoring services for <<Monitoring Length>> through Equifax as described below.

What You Can Do. You can follow the recommendations included with this letter to protect your personal information. We also strongly encourage you to enroll in the credit monitoring and identity monitoring services we are offering through Equifax. To enroll in this service, go to ***www.equifax.com/activate*** or call 866-243-0734 and when prompted for the Activation Code, provide **<<Insert Unique 12-letter Activation Code>>** and follow the steps to receive your credit monitoring services. Your complimentary services will include credit monitoring, fraud alerts, and $1,000,000 in identity theft insurance. The deadline to enroll is **<<Enrollment Deadline>>**.

For More Information: If you have any questions regarding the incident or would like assistance with enrolling in the credit and identity monitoring services, please call 800-658-9182 between 9am to 9pm Eastern Time from Monday to Friday.

Please accept our sincere apologies and know that we deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Gerald R. Salerno

Gerald R. Salerno, Esq.
Aronsohn Weiner Salerno & Kaufman, PC

Enter your Activation Code: <<*ACTIVATION CODE*>>
Enrollment Deadline: *January 31, 2022*

Equifax Credit Watch™ Gold

*Note: You must be over age 18 with a credit file to take advantage of the product

Key Features

- Credit monitoring with email notifications of key changes to your Equifax credit report
- Daily access to your Equifax credit report
- WebScan notifications[1] when your personal information, such as Social Security Number, credit/debit card or bank account numbers are found on fraudulent Internet trading sites
- Automatic fraud alerts[2], which encourages potential lenders to take extra steps to verify your identity before extending credit, plus blocked inquiry alerts and Equifax credit report lock[3]
- Identity Restoration to help restore your identity should you become a victim of identity theft, and a dedicated Identity Restoration Specialist to work on your behalf
- Up to $1,000,000 of identity theft insurance coverage for certain out of pocket expenses resulting from identity theft[4]

Enrollment Instructions

Go to ***www.equifax.com/activate***
Enter your unique Activation Code of **<<*ACTIVATION CODE*>>** then click "Submit" and follow these 4 steps:

1. **Register:**
   Complete the form with your contact information and click "Continue".
   If you already have a myEquifax account, click the 'Sign in here' link under the "Let's get started" header. Once you have successfully signed in, you will skip to the Checkout Page in Step 4
2. **Create Account:**
   Enter your email address, create a password, and accept the terms of use.
3. **Verify Identity:**
   To enroll in your product, we will ask you to complete our identity verification process.
4. **Checkout:**
   Upon successful verification of your identity, you will see the Checkout Page.
   Click 'Sign Me Up' to finish enrolling.

   You're done!
   The confirmation page shows your completed enrollment.
   Click "View My Product" to access the product features.

---

[1] WebScan searches for your Social Security Number, up to 5 passport numbers, up to 6 bank account numbers, up to 6 credit/debit card numbers, up to 6 email addresses, and up to 10 medical ID numbers. WebScan searches thousands of Internet sites where consumers' personal information is suspected of being bought and sold, and regularly adds new sites to the list of those it searches. However, the Internet addresses of these suspected Internet trading sites are not published and frequently change, so there is no guarantee that we are able to locate and search every possible Internet site where consumers' personal information is at risk of being traded.

[2] The Automatic Fraud Alert feature is made available to consumers by Equifax Information Services LLC and fulfilled on its behalf by Equifax Consumer Services LLC.

[3] Locking your Equifax credit report will prevent access to it by certain third parties. Locking your Equifax credit report will not prevent access to your credit report at any other credit reporting agency. Entities that may still have access to your Equifax credit report include: companies like Equifax Global Consumer Solutions, which provide you with access to your credit report or credit score, or monitor your credit report as part of a subscription or similar service; companies that provide you with a copy of your credit report or credit score, upon your request; federal, state and local government agencies and courts in certain circumstances; companies using the information in connection with the underwriting of insurance, or for employment, tenant or background screening purposes; companies that have a current account or relationship with you, and collection agencies acting on behalf of those whom you owe; companies that authenticate a consumer's identity for purposes other than granting credit, or for investigating or preventing actual or potential fraud; and companies that wish to make pre-approved offers of credit or insurance to you. To opt out of such pre-approved offers, visit www.optoutprescreen.com

[4] The Identity Theft Insurance benefit is underwritten and administered by American Bankers Insurance Company of Florida, an Assurant company, under group or blanket policies issued to Equifax, Inc., or its respective affiliates for the benefit of its Members. Please refer to the actual policies for terms, conditions, and exclusions of coverage. Coverage may not be available in all jurisdictions.

Steps You Can Take to Protect Your Personal 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.