LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Jason Cherry
633 W 5th St #4000,
Los Angeles, CA 90071
Jason.Cherry@lewisbrisbois.com
Direct: 213.358.6067

September 13, 2022

VIA EMAIL

Attorney General Brian E. Frosh
Office of the Attorney General
Attn: Security Breach Notification
200 St. Paul Place
Baltimore, MD 21202
Fax: (410) 576-6566
Idtheft@oag.state.md.us

Re: **Notification of Data Security Incident**

Dear Attorney General Frosh:

Lewis Brisbois Bisgaard & Smith LLP represents Elisa Meyer, CPA ("Ms. Meyer") 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

Elisa Meyer is a provider of tax and accounting services located in California.

On or about May 9, 2022, Ms. Meyer learned of suspicious activity in her business email environment. Upon discovery, Ms. Meyer took immediate steps to secure the environment. In addition, Ms. Meyer retained outside cybersecurity experts to conduct an investigation to determine what happened and to identify any information that may have been accessed or acquired without authorization. The forensics firm undertook an extensive review of Ms. Meyer's systems to determine what personal information may have been impacted, the individuals to whom the information pertained, and addresses for these individuals.

On August 1, 2022, Ms. Meyer learned that certain personal information may have been impacted in connection with the incident and worked to provide notification of the incident to potentially impacted individuals out of an abundance of caution.

2. Type of Information and Number of Maryland Residents Involved

The incident involved personal information for four (4) Maryland residents. The information involved differ depending on the individual but may include name, Social Security number, and financial account or routing number.

The affected individuals will be sent 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 September 13, 2022.

3. Measures Taken to Address the Incident

In response to the incident, Elisa Meyer retained cybersecurity experts and launched a forensics investigation to determine the source and scope of the compromise. In addition, Elisa Meyer is in the process of reviewing its current security protocols and adding additional security measures.

As discussed above, Elisa Meyer 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

Elisa Meyer 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 Jason Cherry at Jason.Cherry@lewisbrisbois.com or 213.358.6067.

Sincerely,

Jason Cherry of
LEWIS BRISBOIS BISGAARD &
SMITH LLP

Encl.: Sample Consumer Letter

cpa ElisaMeyer

<<First Name>><<Last Name>>
<<Address1>><<Address2>>
<<City>>,<<State>><<Zip>>

<<Date (Format: Month Day, Year)>>

Subject: Notice of Data <<Variable Text Field 1 Breach / Security Incident>>

Dear <<First Name>> <<Last Name>>,

I am writing to inform you of a recent data security incident experienced by my tax and accounting firm, Elisa Meyer, CPA, that may have impacted your personal information. I take the privacy and security of all personal information within my 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 personal information.

What Happened? On May 9, 2022, I became aware of suspicious activity within my business email environment. In response, I took immediate steps to secure the email environment and promptly launched an investigation into the suspicious activity. In so doing, I engaged an 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. On August 1, 2022, I learned that certain personal information may have been impacted in connection with the incident and worked to provide notification of the incident to potentially impacted individuals. There is no evidence that your data has been misused or that your data is at risk of misuse at this time.

What Information Was Involved? The information potentially impacted in connection with this incident may have included your name as well as your Social Security number and financial account information.

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

Although I have no evidence of the misuse of any potentially impacted information, out of an abundance of caution, I am providing you with information about steps that you can take to help protect your personal information and am offering you complimentary identity protection services through Kroll – a data breach and recovery services expert. These services include 12 months of credit[1] and dark web monitoring, a $1 million identity fraud loss reimbursement policy, and fully managed identity theft recovery services. The deadline to enroll in these services is <<Date>>. Kroll will help to resolve issues if your identity is compromised.

What You Can Do: You can follow the recommendations on the following page to help protect your personal information. I also encourage you to enroll in the complementary services being

[1] To receive credit monitoring services, you must be over the age of 18 and 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.

offered to you through Kroll by using the enrollment code provided in this letter.

How to Activate:

Visit **https://enroll.krollmonitoring.com** to activate and take advantage of your identity monitoring services.

You have until **<<b2b_text_6(activation deadline)>>** to activate your identity monitoring services.

Membership Number: **<<Membership Number s_n>>**

To receive credit monitoring services, you must be over the age of 18 and 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. Please do not discard this letter, as you will need the Membership Number provided above to access services.

For More Information: Further information about how to protect your personal information appears on the following page. If you have questions or need assistance, please call Kroll at 1-877-300-6846. Kroll call center representatives are fully versed on this incident and can answer any questions that you may have.

Please accept my sincere apologies and know that I take this matter very seriously and deeply regret any worry or inconvenience that this may cause you.

Sincerely,

Elisa Meyer, CPA

STEPS YOU CAN TAKE TO HELP PROTECT YOUR INFORMATION

IRS Identity Protection PIN: You can obtain an identity protection PIN (IP PIN) from the IRS that prevents someone else from filing a tax return using your Social Security number. The IP PIN is known only to you and the IRS and helps the IRS verify your identity when you file your electronic or paper tax return. You can learn more and obtain your IP PIN here: https://www.irs.gov/identity-theft-fraud-scams/get-an-identity-protection-pin.

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.

Credit or 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

California Attorney General
P.O. Box 944255
Sacramento, CA 94244-2550
https://oag.ca.gov/privacy
1 800-952-5225

North Carolina Attorney General
9001 Mail Service Center
Raleigh, NC 27699
ncdoj.gov
1-877-566-7226

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.