LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Lindsay B. Nickle
2100 Ross Avenue, Suite 2000
Dallas, Texas 75201
Lindsay.Nickle@lewisbrisbois.com
Direct: 214.722.7141

May 18, 2022

Via Email

Attorney General John Formella
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Phone: (603) 271-3643
Fax: (603) 271-2110

Re: Notice of Data Security Incident

To Whom It May Concern:

Lewis Brisbois Bisgaard & Smith LLP ("Lewis Brisbois") represents Fredette, Sankowski, Woodcock & Co. in connection with a recent data security incident described in greater detail below.

1. **Nature of the security incident.**

During the 2022 tax season, Fredette, Sankowski, Woodcock & Co. became aware of a higher-than-usual number of clients that have experienced unusual activity associated with their bank accounts and/or fraudulent tax filings starting around March 15, 2022. Upon learning about this activity, they engaged independent digital forensics and incident response experts to help determine if their computer network has been impacted or compromised. The investigation has indicated that this activity may be related to a phishing attempt.

On April 13, 2022, Fredette, Sankowski, Woodcock & Co. learned that personal information belonging to certain individuals associated with Fredette, Sankowski, Woodcock & Co. may have been impacted in connection with the incident. Fredette, Sankowski, Woodcock & Co. 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 names, addresses, Social Security numbers, financial account information, and wage and tax filing information.

2. Number of New Hampshire residents affected.

Fredette, Sankowski, Woodcock & Co. notified two New Hampshire residents of this incident via first class U.S. mail on May 12, 2022. A sample copy of the notification letter is included with this correspondence.

3. Steps taken relating to the Incident.

As soon as Fredette, Sankowski, Woodcock & Co. discovered this incident, Fredette, Sankowski, Woodcock & Co. 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. Fredette, Sankowski, Woodcock & Co. 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.

In addition, Fredette, Sankowski, Woodcock & Co. has provided all notified individuals with credit monitoring and identity remediation services and has provided 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.

4. Contact information.

Fredette, Sankowski, Woodcock & Co. 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,

Lindsay B. Nickle of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Sample Notification Letter

Return Mail Processing Center
P.O. Box 6336

Portland, OR 97228-6336

To Enroll, Please visit:
www.equifax.com/activate
Enrollment Code: <<Code>>

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

<<Date>>

Subject: Notice of Data <<Variable Header>>

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

I am writing to inform you about a potential data security incident about which Fredette, Sankowski, Woodcock & Co. has become aware. Fredette, Sankowski, Woodcock & Co. takes the privacy and security of all personal information within its possession very seriously. Because this potential data security incident may impact your personal information, we are sending you this letter about what we have learned about and providing you with steps you can take to help protect your personal information.

What Happened? During the 2022 tax season, Fredette, Sankowski, Woodcock & Co. became aware of a higher-than-usual number of clients that have experienced unusual activity associated with their bank accounts and/or fraudulent tax filings. Upon learning about this activity, we engaged independent digital forensics and incident response experts to help us determine if our computer network has been impacted or compromised.

Our investigation has indicated that this activity may be related to a phishing attempt. As a customer service to our valued clients, we are contacting you to notify you about the suspicious and fraudulent activity we have learned about, provide information about how you can protect your personal information, and to offer you <<12 / 24>> months of credit monitoring and identity protection services at no cost to you.

What Information Was Involved? The personal information that has been misused in connection with the activity we have learned about includes names, addresses, Social Security numbers, financial account information, and wage and tax filing information.

What Are We Doing? As soon as we began receiving reports of fraudulent activity, we took the steps described above. In addition, we are providing you with the following information and resources:

- We have notified the IRS of the situation to attempt to prevent fraudulent activity. We will continue to provide the IRS with whatever cooperation is necessary to protect you and ensure you receive any tax refund you may be due.
- We are implementing several enhanced security measures to safeguard personal information in our possession and minimize the likelihood of a similar event from occurring in the future.
- We are providing you with information about steps that you can take to help protect your personal information and are offering you complimentary identity protection services through Epiq – a data breach and recovery services expert. These services include <<12 / 24>> months of Equifax Credit Watch – Gold which includes credit monitoring with email notification, access to credit report, WebScan notifications if your data is used, and identity theft insurance coverage for certain out of pocket expenses resulting from identity theft. The deadline to enroll in these services is <<Enrollment Deadline>>. With this protection, Epiq 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. We also encourage you to enroll in the complimentary services being offered to you through Epiq by using the enrollment code provided above.

- You should follow the guidelines included with this letter for an overview of steps you can take, including how to place a fraud alert on your credit report, or place a security freeze on your credit file.
- You should review all financial account statements carefully and if you notice any suspicious activity, contact your financial institution and notify law enforcement.
- You should be especially aware of any requests, calls, letters or other questions about any of your personal accounts. If you receive some type of unexpected request for personal information, do not provide any information and instead contact the entity requesting the information to validate whether the request was legitimate.
- You may receive a Form 5071C letter from the IRS. If you receive a Form 5071C letter, please follow the instructions in the letter to verify your identity with the IRS. The IRS will be assigning individual PIN numbers to taxpayers who have received a Form 5071C letter. Those PIN numbers are sent out by mail from the IRS. Only those who are sent the letter are assigned PIN numbers. If you have questions about how having a PIN number impacts your tax filing, please contact us. In addition, you may be required to complete the IRS Form 14039 Identity Theft Affidavit. We will assist you with this process as well.
- You may receive a Form 12C letter from the IRS. If you receive a Form 12C letter, please follow the instructions and respond accordingly by mail or fax. If you have questions regarding the letter or response, please contact us and we will assist you with this process.

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 Epiq at **855-614-1706** from 8:00 A.M. to 8:00 P.M. Central Time, Monday through Friday (excluding holidays).

Please know that Fredette, Sankowski, Woodcock & Co. takes this situation very seriously and will assist you as needed.

Sincerely,

Brian Fredette, President
Fredette, Sankowski, Woodcock & Co.

Jillian Woodcock, Vice President
Fredette, Sankowski, Woodcock & Co.

Enter your Activation Code: *<ACTIVATION CODE>*
Enrollment Deadline: *<DEADLINE MMMM DD, YYYY>*

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 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.