LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Alyssa R. Watzman
1700 Lincoln Street, Suite 4000
Denver, Colorado 80203
Alyssa.Watzman@lewisbrisbois.com
Direct: 720.292.2052

June 2, 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:

Lewis Brisbois Bisgaard & Smith LLP ("Lewis Brisbois") represents Ian Martin PBC ("Ian Martin") in connection with a recent data security incident described in greater detail below.

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

On March 23, 2022, Ian Martin detected unusual activity within its network involving the identification of a suspicious file stored on a company server. In response, Ian Martin took immediate steps to secure its environment and promptly engaged an independent digital forensics and incident response firm to determine what happened and identify any information that may have been accessed or acquired without authorization. As a result of that investigation, Ian Martin learned that personal information of certain individuals may have been accessed or acquired without authorization between March 15, 2022 and March 22, 2022. Upon learning this, Ian Martin undertook a comprehensive review of the potentially impacted data to identify the individuals whose information may have been involved and to gather up-to-date contact information for purposes of providing notification. Ian Martin completed that process on May 3, 2022 and promptly arranged for notification letters to be sent.

The information that may have been accessible by the malicious actor(s) responsible for this incident includes names and Social Security numbers.

2. **Number of Maine residents affected.**

Ian Martin will be notifying three (3) Maine residents of this incident via first class U.S. mail on June 2, 2022. A sample copy of the notification letter is included with this correspondence.

3. **Steps taken relating to the Incident.**

As soon as Ian Martin discovered this incident, Ian Martin took steps to secure its network

environment and launched an investigation to determine what happened and whether personal information had been accessed or acquired without authorization. Ian Martin has also implemented additional safeguards to help ensure the security of its environment and reduce the risk of a similar incident occurring in the future. Ian Martin also reported this incident to the Federal Bureau of Investigation and will cooperate with authorities in any investigation.

Ian Martin has established a toll-free call center through Kroll, a leader in risk mitigation and response, to answer any questions about the incident and address related concerns. In addition, while Ian Martin is not aware of the misuse of any information as a result of this incident, out of an abundance of caution, Ian Martin is also providing complimentary identity protection services to notified individuals.

4. Contact information.

Ian Martin remains dedicated to protecting the personal information in its control. If you have questions or need additional information, please do not hesitate to contact me.

Best regards,

Alyssa R. Watzman
LEWIS BRISBOIS BISGAARD & SMITH LLP

Enclosure: Sample Notification Letter

IAN MARTIN

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

<<first_name>> <<middle_name>> <<last_name>> <<suffix>>
<<address_1>>
<<address_2>>
<<city>>, <<state_province>> <<postal_code>>
<<country>>

<<b2b_text_1(Subject: Notice of Data (Breach or Security Incident)>>

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>,

I am writing to inform you of a recent data security incident experienced by Ian Martin PBC ("Ian Martin") that may have affected your personal information. Please read this letter carefully as it contains information regarding the incident and steps you can take to help protect your personal information.

What Happened: On March 23, 2022, Ian Martin detected unusual activity after identifying a suspicious file stored on a company server. In response, Ian Martin immediately took steps to ensure the security of its network environment and launched an investigation. Ian Martin enlisted an incident response firm to determine what happened and whether any Ian Martin data was impacted. As a result of the investigation, Ian Martin learned that an unknown actor may have accessed or acquired certain personal information stored on an internal file server between March 15, 2022 and March 22, 2022. Ian Martin then undertook a thorough review of the data to identify individuals whose information may have been involved and to gather up-to-date address information for purposes of notification. Ian Martin completed that process on May 3, 2022 and promptly arranged for this notification to be sent.

What Information Was Involved: The information that was potentially impacted may have included your name as well as your <<b2b_text_2(data elements)>>. Please note that Ian Martin has no evidence that any of this information has been misused.

What Are We Doing: As soon as Ian Martin discovered this incident, we immediately implemented measures to increase security and launched an investigation as described above. Ian Martin also notified law enforcement agencies and will cooperate with authorities so that the perpetrator(s) may be held accountable.

Although Ian Martin has no evidence that any potentially impacted information was misused, out of an abundance of caution, we are offering you complimentary identity protection services through Kroll, a national leader in identity theft protection. Your identity monitoring services include 12 months of Credit Monitoring, Web Watcher, Fraud Consultation, and Identity Theft Restoration, and $1 million Identity Fraud Loss Reimbursement. With this protection, Kroll will help you resolve issues if your identity is compromised.[1] Ian Martin is also providing you with information, included on the following page, about steps you can take to help protect your personal information.

What You Can Do: Ian Martin encourages you to follow the recommendations on the following page and to activate the complementary services being offered to you through Kroll by using the activation code provided below. With this protection, Kroll will help to resolve issues if your identity is compromised.

[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.

How to Activate:

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

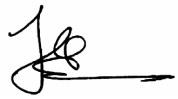
You have until <<b2b_text_6(activation deadline)>> to activate your identity monitoring services.

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

For More Information: Further information about how to help protect your personal information can be found on the following page. If you have questions or need assistance, please call Kroll at 1-???-???-????, Monday through Friday from 8:00 a.m. to 5:30 p.m. Central Time, excluding some major U.S. holidays. Kroll call center representatives are fully versed on this incident and can answer any questions that you may have.

Ian Martin takes the privacy and security of all personal information within its possession very seriously. Your trust is very important to us; please accept my sincere apologies for any concern or inconvenience that this has caused you.

Sincerely,



Tim Masson, CEO
Ian Martin PBC

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

California Attorney General
California Department of Justice
Attn: Public Inquiry Unit
P.O. Box 944255
Sacramento, ca 9424402559

Texas Attorney General
Consumer Protection Division
P.O. Box 12548
Austin, TX 78711-2548

Florida Attorney General
Department of Legal Affairs
State of Florida
PL-01 The Capitol
Tallahassee, FL 3239901059

Massachusetts Attorney General
Consumer Protection Division
ATTN: Data Breach Notification
One Ashburton Place
Boston, MA 02108

Michigan Attorney General
Consumer Protection Division
G. Mennen Williams Building
525 W Ottawa Street
P.O. Box 30213
Lansing, MI 48909

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.

KROLL

TAKE ADVANTAGE OF YOUR IDENTITY MONITORING SERVICES

You have been provided with access to the following services from Kroll:

Single Bureau Credit Monitoring

You will receive alerts when there are changes to your credit data—for instance, when a new line of credit is applied for in your name. If you do not recognize the activity, you'll have the option to call a Kroll fraud specialist, who will be able to help you determine if it is an indicator of identity theft.

$1 Million Identity Fraud Loss Reimbursement

Reimburses you for out-of-pocket expenses totaling up to $1 million in covered legal costs and expenses for any one stolen identity event. All coverage is subject to the conditions and exclusions in the policy.

Web Watcher

Web Watcher monitors internet sites where criminals may buy, sell, and trade personal identity information. An alert will be generated if evidence of your personal identity information is found.

Fraud Consultation

You have unlimited access to consultation with a Kroll fraud specialist. Support includes showing you the most effective ways to protect your identity, explaining your rights and protections under the law, assistance with fraud alerts, and interpreting how personal information is accessed and used, including investigating suspicious activity that could be tied to an identity theft event.

Identity Theft Restoration

If you become a victim of identity theft, an experienced Kroll licensed investigator will work on your behalf to resolve related issues. You will have access to a dedicated investigator who understands your issues and can do most of the work for you. Your investigator will be able to dig deep to uncover the scope of the identity theft, and then work to resolve it.

Kroll's activation website is only compatible with the current version or one version earlier of Chrome, Firefox, Safari and Edge.

To receive credit 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.