LEWIS BRISBOIS

LEWIS BRISBOIS BISGAARD & SMITH LLP

Kamran Salour
650 Town Center Drive, Suite 1400
Costa Mesa, California 92626
Kamran.Salour@lewisbrisbois.com
Direct: 714.966.3145

June 14, 2021

VIA EMAIL

Attorney General Gordon MacDonald
Office of the Attorney General
Consumer Protection Bureau
33 Capitol Street
Concord, NH 03301
Phone: (603) 271-3643
Fax: (603) 271-2110
Email: DOJ-CPB@doj.nh.gov

Re: **Notice of Data Security Incident**

Dear Attorney General MacDonald:

Lewis Brisbois Bisgaard & Smith LLP represents Pickard Chilton Architects ("Pickard Chilton") 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 New Hampshire's data breach notification statute, N.H. Rev. Stat. §§ 359-C:19 - C:21.

1. **Nature of the Incident**

On March 5, 2021, Pickard Chilton became aware of unusual activity within its network environment and discovered that it had been the victim of data encryption by an unknown actor. Upon discovering this activity, it took immediate steps to secure our environment and launched an investigation with the assistance of leading independent digital forensics and cybersecurity experts. The investigation determined that certain Pickard Chilton data may have been accessed or downloaded as a result of this incident.

As a result, Pickard Chilton promptly undertook a review of the affected data in order to identify any individuals whose personal information was within the potentially affected data.

2. **Type of Information and Number of New Hampshire Residents Involved**

The incident involved personal information for approximately 1 New Hampshire residents. The information involved in the incident may include Date of Birth, Social Security Number.

The affected individuals will receive a letter notifying them of the incident and providing steps they can take to protect their personal information. The notification letter will be sent via USPS First Class Mail on June 16, 2021.

3. Measures Taken to Address the Incident

Pickard Chilton has taken steps in response to this incident to minimize the likelihood of similar incidents occurring in the future. Those steps include deployment of an advanced threat detection tool with twenty-four hour active monitoring by a cybersecurity operations team, resetting all user passwords within the environment, and implementing multi-factor authentication (MFA). In addition, out of an abundance of caution, Pickard Chilton is offering the potentially affected individuals credit monitoring, identity protection services, and identity theft insurance at no cost.

4. Contact information.

Pickard Chilton remains dedicated to the protection of all personal information within its control. If you have any questions or need additional information relating to this incident, please do not hesitate to contact me at Kamran.Salour@lewisbrisbois.com. Please include Shaun G. Goodfriend, Shaun.Goodfriend@lewisbrisbois.com, on all correspondence pertaining to this matter as well.

Sincerely,

/s/ Kamran Salour

Kamran Salour of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl.: Sample Consumer Notification Letter

To Enroll, Please Call:
_____
Or Visit:
_____
Enrollment Code:
<<XXXXXXXX>>

Logo/Client Name
C/O Kroll
<<Return Address>>
<<City>>, <<State>> <<Zip>>

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

Re: Notice of Data Security Incident

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

Please know that the privacy and security of Pickard Chilton employees' information is paramount, and the firm takes it protection very seriously. That is why I write to inform you of a data security incident that *may* have affected some of your personal information. This letter is to notify you of the incident, offer you complimentary credit and identity monitoring services out of an abundance of caution, and inform you about steps that you can take to protect yourself.

What Happened? On March 5, 2021, Pickard Chilton learned that some of our employees did not receive the deposit of their paychecks. Pickard Chilton subsequently retained an independent forensic firm to investigate the situation. Their investigation determined that an unknown threat actor accessed our Office 365 environment without authorization in order to redirect some payments to a separate account. There is no evidence to indicate, let alone suggest that any of your information has been misused; the threat actor's goal was to misdirect payments. Nonetheless, because we value our employees, we have elected to provide you with access to complementary identity monitoring protection services to help ease any concerns you may have about this incident.

What Information Was Involved? The personal information involved may have included <<VARIABLE TEXT2>>.

What We Are Doing? In addition to hiring outside experts to investigate, Pickard Chilton contacted the FBI to investigate. We have also enabled additional security features for our digital environment to help reduce the likelihood of such an incident happening again. We are also offering <<VARIABLE TEXT2>> months of credit and identity restoration services at no cost to you and providing you with additional information about steps that you can take to further protect your information.

What You Can Do? We invite you to follow the recommendations on the following page to protect your information. We also encourage you to enroll in the identity theft protection services we are offering through Kroll, a national leader in identity protection services. The identity protection services include <<VARIABLE TEXT2>> months of credit monitoring, and fully managed identity theft recovery services. In order to receive credit monitoring services, you must have established credit in the US, have a Social Security number in your name, and have a US residential address associated with your credit file. You can enroll in free Kroll identity protection services by calling _____ or going to _____ and using the Enrollment Code provided above. Kroll representatives are available to assist you Monday through Friday from 9:00 a.m. to 9:00 p.m. Eastern Time. Please note the deadline to enroll is _____.

For More Information. Detailed instructions for enrollment are on the enclosed "Recommended Steps" document. Please note that you will need to reference the enrollment code at the top of this letter when calling or enrolling online, so please do not discard this letter. Please call _____ or go to _____ for assistance or for any additional questions you may have.

Thank you for your understanding of this matter. Please let me know if I can be of assistance.

Sincerely,

Jovan K. Rhodes
4837-0439-4730.2

STEPS YOU CAN TAKE TO 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 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:

TransUnion	**Experian**	**Equifax**	**Free Annual Report**
P.O. Box 1000	P.O. Box 2002	P.O. Box 740241	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30374	Atlanta, GA 30348
1-800-916-8800	1-888-397-3742	1-866-349-5191	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	annualcreditreport.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 90 days. 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: Under U.S. law, 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. The three credit reporting agencies are listed above, and you should contact them to establish a security freeze. 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	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903
consumer.ftc.gov, and	oag.state.md.us	ncdoj.gov	http://www.riag.ri.gov
www.ftc.gov/idtheft	1-888-743-0023	1-877-566-7226	401-274-4400
1-877-438-4338			

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 http://files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.