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

December 10, 2020

VIA ELECTRONIC MAIL
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:

We represent Fein, Such, Kahn & Shepard, P.C. ("FSKS"), a full service law firm that provides services to clients located in New Jersey, New York, and Pennsylvania. This letter is being sent because the personal information of certain New Hampshire residents may have been affected by a data security incident experienced by FSKS. The incident may have involved unauthorized access to such residents' names as well as such residents' address, date of birth, financial account information, payment card information, driver's license or other government identification number, Social Security number, passport number, individual taxpayer identification number, and/or online credentials.

On May 6, 2020, FSKS detected unusual activity within one FSKS employee email account. Upon discovering this activity, FSKS immediately took steps to secure the account and launched an investigation with the assistance of an independent forensic firm to determine what happened and whether sensitive information was accessed or acquired without authorization as a result. The forensic firm later confirmed that two FSKS employee email accounts potentially containing sensitive information were accessed without authorization and undertook a review of the contents of those accounts. On November 12, 2020, FSKS learned that those employee email accounts contained some personal information belonging to New Hampshire residents which may have been accessed by an unauthorized actor as a result of this incident. FSKS then worked diligently to provide notification.

FSKS notified three potentially impacted New Hampshire residents of this incident via the attached sample letter on December 10, 2020. In so doing, FSKS offered notified individuals complimentary credit monitoring and identity theft restoration services through Kroll.

Please contact me should you have any questions.

Sincerely,

/s/ Kamran Salour

Kamran Salour of
LEWIS BRISBOIS BISGAARD & SMITH LLP

Encl.: Sample Consumer Notification Letter

FSKS

FEIN, SUCH, KAHN & SHEPARD, P.C.

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

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

Re: Notice of Data Breach

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

We are writing to inform you of a data security incident experienced by Fein, Such, Kahn & Shepard, P.C. ("FSKS") that may have affected your personal information. FSKS is not aware of the misuse of any potentially impacted information. Nonetheless, the privacy and security of your information is extremely important to FSKS. That is why we are writing to notify you of this incident, to offer you complimentary credit monitoring and identity theft restoration services, and to inform you about steps that can be taken to help protect your personal information.

What Happened? On May 6, 2020, we detected unusual activity within one FSKS employee email account. Upon discovering this activity, we immediately took steps to secure the account. We engaged an independent forensic firm to determine what happened and whether sensitive information was accessed or acquired without authorization. The forensic firm later confirmed that two FSKS employee email accounts potentially containing sensitive information were accessed without authorization and undertook a review of the contents of those accounts. On November 12, 2020, we learned that those FSKS employee email accounts contained some of your personal information that may have been accessed by an unauthorized actor as a result of this incident. We then worked diligently to provide notification.

Please note that this unauthorized access was limited to information transmitted via email only; there was no unauthorized access to any other information systems. In addition, FSKS is not aware of the misuse of any potentially impacted information.

What Information Was Involved? The information impacted in connection with this incident may have included your name as well as your address, date of birth, financial account information, payment card information, driver's license or other government identification number, Social Security number, passport number, individual taxpayer identification number, and/or online credentials.

What We Are Doing. As soon as we discovered this incident, we took the above steps. Additionally, because we take the confidentiality of all information within our possession very seriously, we took steps to enhance the security of our email environment to minimize the likelihood of similar incidents happening again. Finally, out of an abundance of caution, we are offering you complimentary identity monitoring services through Kroll, a global leader in risk mitigation and response. These services include twelve months of Credit Monitoring, $1 Million Identity Fraud Loss Reimbursement, Fraud Consultation, and Identity Theft Restoration.

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

*You have until **March 12, 2021** to activate your identity monitoring services.*

Membership Number: **<<Member ID>>**

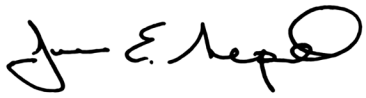
To receive these services, you must be over the age of 18, have established credit in the United States, have a Social Security number in your name, and have a United States residential address associated with your credit file.

What You Can Do. We recommend that you activate your complimentary Kroll services provided above. We also recommend that you review the guidance included with this letter about how to help protect your personal information.

For More Information. If you have questions or need assistance, please contact Kroll at 1-833-971-3262, Monday through Friday from 9:00 a.m. to 6:30 p.m. Eastern Standard Time. Kroll representatives are fully versed on this incident and can answer any questions you may have regarding the protection of your personal information.

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

Sincerely,



James E. Shepard, Esq.
Managing Shareholder
Fein, Such, Kahn & Shepard, P.C.

Steps You Can Take to Further 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 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 can print this form at www.annualcreditreport.com/cra/requestformfinal.pdf. 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 9532	P.O. Box 105851	P.O. Box 105281
Chester, PA 19016	Allen, TX 75013	Atlanta, GA 30348	Atlanta, GA 30348
1-800-916-8800	1-888-397-3742	1-800-525-6285	1-877-322-8228
www.transunion.com	www.experian.com	www.equifax.com	www.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 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 www.annualcreditreport.com.

Security Freeze: You have the right to put a security freeze on your credit file. 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. There is no charge to place, lift or remove the security freeze. 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 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. Residents of Maryland, North Carolina, and Rhode Island, and Washington, DC can obtain more information from their Attorneys General using the contact information below.

Federal Trade Commission	**Maryland Attorney General**	**North Carolina Attorney General**	**Rhode Island Attorney General**	**Washington D.C. Attorney General**
600 Pennsylvania Ave, NW	200 St. Paul Place	9001 Mail Service Center	150 South Main Street	441 4th Street, NW
Washington, DC 20580	Baltimore, MD 21202	Raleigh, NC 27699	Providence, RI 02903	Washington, DC 20001
consumer.ftc.gov, and www.ftc.gov/idtheft	https://oag.state.md.us	https://ncdoj.gov	http://www.riag.ri.gov	https://oag.dc.gov/
1-877-438-4338	1-888-743-0023	1-877-566-7226	401-274-4400	202-727-3400

You also have certain rights under the Fair Credit Reporting Act (FCRA), including: 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 others. For more information about the FCRA, and your rights pursuant to the FCRA, please visit files.consumerfinance.gov/f/201504_cfpb_summary_your-rights-under-fcra.pdf.

Kroll | A Division of DUFF&PHELPS

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 will 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.

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.