523 W. 6th Street, Suite 516
Los Angeles, CA 90014

Zweiback Fiset & Coleman LLP

213.266.5170
zfclaw.com

April 8, 2022

VIA MAIL

New Hampshire Department of Justice
Office of the Attorney General
33 Capitol Street
Concord, NH 03301

Re: Data Security Breach Notification

To Whom it May Concern:

This firm represents Kingsley & Kingsley Lawyers (KKL), an employment law firm located at 16133 Ventura Blvd Suite 1200, Encino, CA 91436. On or about August 21-22, 2021, an unknown attacker or attackers conducted a ransomware attack on two of KKL's computer servers. On August 22, 2021, Kingsley IT staff physically disconnected the two servers from the network and powered them down, thus disrupting the attack.

Although the investigation is ongoing, and current understanding of the attack may change as KKL continues its analysis, it appears that seven New Hampshire residents' Personally Identifying Information (PII) may have been accessed without authorization by the attackers. The impacted information may have included first and last name and social security number. KKL has sent a notification letter to the potentially affected individuals on or about April 1, 2022 via mail. A copy of the form notification letter is enclosed.

Upon learning of the issue, KKL immediately commenced a thorough investigation, which has included forensic investigators and expert legal counsel, all cybersecurity professionals experienced in handling incidents such as the attack KKL suffered. KKL also has been consulting with appropriate law enforcement authorities and, as provided for in applicable law, has delayed its notification of this incident while KKL conducted its investigation and worked with law enforcement.

KKL is committed to maintaining the privacy of sensitive information in its possession and has taken many precautions to safeguard it. KKL continually evaluates and modifies its practices and internal controls to enhance the security and privacy of sensitive information in its possession. Since this incident, KKL has implemented additional technical, administrative, and personnel

safeguards to protect information and has educated its employees on identifying and responding to security incidents.

If you have any further questions regarding this incident, please contact me directly at michael.zweiback@zfclaw.com or 213-266-5171.

Sincerely,

Michael Zweiback

Michael Zweiback

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

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

IMPORTANT INFORMATION PLEASE REVIEW CAREFULLY

NOTICE OF DATA BREACH

Dear <<first_name>> <<middle_name>> <<last_name>> <<suffix>>:

We are writing with important information regarding an unfortunate security incident. The privacy and security of the personal, client, and other sensitive information we maintain is of the utmost importance to Kingsley & Kingsley Lawyers (KKL). As such, we wanted to provide you with information about the incident, explain the services we are making available to you, and let you know that we continue to take significant measures to protect your information.

What Happened

On or about August 21-22, 2021, an unknown attacker or attackers conducted a ransomware attack on two of KKL's computer servers. On August 22, 2021, Kingsley IT staff physically disconnected the two servers from the network and powered them down, thus disrupting the attack. Although our investigation is ongoing and our current understanding of the attack may change as we continue our analysis, it appears that some of your Personally Identifying Information (PII) may have been accessed without authorization by the attackers.

What Information Was Involved

The impacted information may have included some of your personal [and/or client] information, including first and last name, and Social Security number.

What We Are Doing

Upon learning of the issue, we immediately commenced a thorough investigation, which has included forensic investigators and expert legal counsel, all cybersecurity professionals experienced in handling incidents such as the attack we suffered. We also have been consulting with appropriate law enforcement authorities, as provided for in applicable law, and have delayed our notification of this incident while we conducted our investigation and worked with law enforcement.

What You Can Do

To help relieve concerns and restore confidence following this incident, we have secured the services of Kroll to provide identity monitoring at no cost to you for one year. Kroll is a global leader in risk mitigation and response, and their team has extensive experience helping people who have sustained an unintentional exposure of confidential data. Your identity monitoring services include Credit Monitoring, Fraud Consultation, and Identity Theft Restoration.

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

You have until <<b2b_text_6 (Activation Date)>> to activate your identity monitoring services.

Membership Number: <<Membership Number s_n>>

For more information about Kroll and your Identity Monitoring services, you can visit info.krollmonitoring.com. Additional information describing your services is included with this letter.

This letter also provides other precautionary measures you can take to help protect your personal information, including placing a fraud alert and/or security freeze on your credit files, and/or obtaining a free credit report. Additionally, you should always remain vigilant in reviewing your account statements for fraudulent or irregular activity on a regular basis.

For More Information

Please accept our sincere apologies that this incident occurred. We are committed to maintaining the privacy of sensitive information in our possession and have taken many precautions to safeguard it. We continually evaluate and modify our practices and internal controls to enhance the security and privacy of sensitive information in our possession. Since this incident, we have implemented additional technical, administrative, and personnel safeguards to protect information and have educated our employees on identifying and responding to security incidents.

If you have any further questions regarding this incident, please call our dedicated and confidential response line that we have set up to respond to questions at 818-990-8300. This response line is staffed with professionals familiar with this incident and knowledgeable on what you can do to help protect against misuse of your information. The response line is available Monday through Friday, 9 a.m. to 6 p.m. Pacific Time.

Sincerely,

Kingsley & Kingsley Lawyers

ADDITIONAL RESOURCES

Contact information for the three nationwide credit reporting agencies:

Equifax, PO Box 740241, Atlanta, GA 30374, www.equifax.com, 1-800-685-1111

Experian, PO Box 2104, Allen, TX 75013, www.experian.com, 1-888-397-3742

TransUnion, PO Box 2000, Chester, PA 19016, www.transunion.com, 1-800-888-4213

Free Credit Report. It is recommended that you remain vigilant by reviewing account statements and monitoring your credit report for unauthorized activity, especially activity that may indicate fraud and identity theft. You may obtain a copy of your credit report, free of charge, once every 12 months from each of the three nationwide credit reporting agencies.

To order your annual free credit report please visit **www.annualcreditreport.com** or call toll free at **1-877-322-8228.**

You can also order your annual free credit report by mailing a completed Annual Credit Report Request Form (available from the U.S. Federal Trade Commission's ("FTC") website at www.consumer.ftc.gov) to:

Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281.

Fraud Alerts. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud—an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have been, or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft and you have the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by contacting any of the three national credit reporting agencies.

Security Freeze. You have the ability to place a security freeze, also known as a credit freeze, on your credit report free of charge.

A security freeze is intended to prevent credit, loans and services from being approved in your name without your consent. To place a security freeze on your credit report, you may use an online process, an automated telephone line, or submit a written request to any of the three credit reporting agencies listed above. The following information must be included when requesting a security freeze (note that, if you are requesting a credit report for your spouse, this information must be provided for him/her as well): (1) full name, with middle initial and any suffixes; (2) Social Security number; (3) date of birth; (4) current address and any previous addresses for the past 5 years; and (5) any applicable incident report or complaint with a law enforcement agency or the Registry of Motor Vehicles. The request must also include a copy of a government-issued identification card and a copy of a recent utility bill or bank or insurance statement. It is essential that each copy be legible, and display your name, current mailing address, and the date of issue.

Federal Trade Commission and State Attorneys General Offices. If you believe you are the victim of identity theft or have reason to believe your personal information has been misused, you should immediately contact the Federal Trade Commission and/or the Attorney General's office in your home state. You may also contact these agencies for information on how to prevent or minimize the risks of identity theft.

You may contact the **Federal Trade Commission**, Consumer Response Center, 600 Pennsylvania Avenue, NW, Washington, DC 20580, www.ftc.gov/bcp/edu/microsites/idtheft/, 1-877-IDTHEFT (438-4338).

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.

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.