Holland & Knight

1180 West Peachtree Street, Suite 1800 | Atlanta, GA 30309 | T 404.817.8500 | F 404.881.0470
Holland & Knight LLP | www.hklaw.com

Bess Hinson
+1 404-817-8527
Bess.Hinson@hklaw.com

September 30, 2022

Via Certified Mail

Office of Attorney General
33 Capitol Street
Concord, New Hampshire 03301

Re: Data Security Incident Notification

Dear Attorney General Formella:

I'm writing on behalf of Baycorp Holdings Ltd., ("Baycorp") to inform you of a data security incident that affects New Hampshire residents. On or around April 6, 2022, Baycorp detected unusual activity on its network. In response to this incident, Baycorp conducted a thorough forensic analysis and investigation. After containing, and eliminating the unauthorized individual's(s') access to its systems, Baycorp implemented additional security measures to further fortify its network's security measures and protocols.

However, an unauthorized individual(s) may still have been able to obtain from the network the personal data of approximately eight (8) residents of New Hampshire, such as name, partial or full social security number, driver's license number, passport number, partial or full payment card information, financial account number, health insurance ID number, and email with security key or password.

Baycorp maintains written privacy and security policies and procedures with respect to personal information collected. Baycorp has taken steps to further strengthen and harden the security of systems in its network, including enhancing administrative and technical safeguards. These administrative and technical safeguards include but are not limited to the following: expanding the use of multi-factor authentication, more frequent and rigorous training of employees on avoiding phishing attempts, additional filtering of malicious links and impersonation protection policies, and enhancing network monitoring.

On September 29, 2022, we mailed the notification letters to the affected New Hampshire residents. Baycorp has established a dedicated call center service to assist affected residents with questions and is offering complimentary access to 12 months of identity theft protection services through Kroll Essential Monitoring Services.

Sincerely yours,

HOLLAND & KNIGHT LLP

Elizabeth ("Bess") K. Hinson

BH

<<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 security incident at <<b2b_text_1 (business name - full)>> ("the Company" or "we"), the steps we are taking to protect you following the incident, and the steps you can take to protect yourself.

What Happened

On or around April 6, 2022, we detected unusual activity on our network. Upon discovery of the unusual activity, we promptly removed access to all systems in our data center and secured the network to block, contain and eliminate the unauthorized individual's(s') access to our systems and engaged a cybersecurity firm to assist with investigating the nature and scope of the incident and remediating any potential negative impact. Through the investigation, we identified unauthorized access to and/or acquisition of certain files on our corporate network on or around April 6, 2022. We conducted a thorough review of these files to identify the individuals whose information was contained in the files and additional research to locate and verify the addresses for these individuals. We completed this process in August 2022, and determined that some of your information was included in the files.

What Information Was Involved

Based on our investigation, we believe that an unauthorized individual(s) may have obtained personal data about you and/or your dependent(s) that was collected in the course of your relationship with us. This information may include your <<b2b_text_2 ("name" and impacted data)>>.

What We Are Doing

In response to this incident, we conducted a thorough forensic analysis and investigation with the assistance of IT security experts. After blocking, containing, and eliminating the unauthorized individual's(s') access to our systems, the Company implemented additional security measures to further fortify its network's security measures and protocols, including enhancing administrative and technical safeguards and instituting more frequent and rigorous security training.

Additionally, to assist you in monitoring your accounts, 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 (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.

What You Can Do

As always, we recommend you be on the alert for suspicious activity related to your financial accounts and credit reports. We encourage you to regularly monitor your statements and records to ensure there are no transactions or other activities that you did not initiate or authorize. You may file a police report regarding this incident. For more information on how to protect against identity theft, please review the enclosed "Additional Resources" section included with this letter. This section describes additional steps you can take to help protect your identity, including recommendations by the Federal Trade Commission regarding identity theft protection and details on how to place a fraud alert or a security freeze on your credit file.

For More Information

Please be assured that we are committed to helping you protect your personally identifiable information and identity and ensuring that your information is safe and secure. We regret this incident and apologize for any concern it may have caused you.

If you have further questions regarding this matter, please do not hesitate to call (855) 926-1126 Monday through Friday, from 8:00 am to 5:30 pm Central Time, excluding some U.S. holidays.

Sincerely,

<<b2b_text_3 (business name - short)>>

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.

For Colorado, Georgia, Maine, Maryland, Massachusetts, New Jersey, Puerto Rico, and Vermont residents: You may obtain one or more (depending on the state) additional copies of your credit report, free of charge. You must contact each of the credit reporting agencies directly to obtain such additional report(s).

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).

For Maryland residents: You may contact the Maryland Office of the Attorney General, Consumer Protection Division, 200 St. Paul Place, Baltimore, MD 21202, www.oag.state.md.us, 1-888-743-0023.

For North Carolina residents: You may contact the North Carolina Office of the Attorney General, Consumer Protection Division, 9001 Mail Service Center, Raleigh, NC 27699-9001, www.ncdoj.gov, 1-877-566-7226.

For New York residents: The Attorney General may be contacted at: Office of the Attorney General, The Capitol, Albany, NY 12224-0341; 1-800-771-7755; https://ag.ny.gov/.

For Connecticut residents: You may contact the Connecticut Office of the Attorney General, 165 Capitol Avenue, Hartford, CT 06106, 1-860-808-5318, www.ct.gov/ag.

For Massachusetts residents: You may contact the Office of the Massachusetts Attorney General, 1 Ashburton Place, Boston, MA 02108, 1-617-727-8400, www.mass.gov/ago/contact-us.html

Reporting of identity theft and obtaining a police report.

For Iowa residents: You are advised to report any suspected identity theft to law enforcement or to the Iowa Attorney General.

For Massachusetts residents: You have the right to obtain a police report if you are a victim of identity theft.

For Oregon residents: You are advised to report any suspected identity theft to law enforcement, the Federal Trade Commission, and the Oregon Attorney General.

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.