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

<<FIRST_NAME>> <<MIDDLE_NAME>> <<LAST_NAME>> <<SUFFIX>>
<<ADDRESS_1>>
<<ADDRESS_2>>
<<CITY>>, <<STATE_PROVINCE>> <<POSTAL_CODE>>
<<COUNTRY>>

NOTICE OF SECURITY INCIDENT

Dear <<first_name>> <<last_name>>,

On behalf of Doyon, Limited, we are writing to inform you about a security event that involved personal information, as defined under the law of the state you live in, about you.

WHAT HAPPENED

On or about April 2, 2024, we discovered that on or about April 1, 2024, an unauthorized actor or actors accessed and acquired files from Doyon's IT systems. We initiated an investigation, retained an outside incident response company, and notified law enforcement. We subsequently conducted a review with the assistance of external experts to determine if personal information was included in the affected files. The investigation and review have been detailed and complicated processes.

We take the security of your personal information very seriously and wanted to bring this to your attention. We also want to apologize for any inconvenience this may cause you.

WHAT INFORMATION WAS INVOLVED

Through our investigation, we have determined that the personal information involved in the incident may include your: <<b2b_text_1 (DataElements)>><<b2b_text_2(DataElementsCont.)>>.

WHAT WE ARE DOING

We initiated an investigation as soon as we learned of these issues to assess and remediate the incident. We have enhanced network security, reported to law enforcement, and implemented additional security measures to further protect our systems.

Upon learning about the event, we promptly took steps to block the unauthorized actor(s) access to Doyon networks; investigate the potential scope of the event, including searching for evidence of other incidents that may have compromised the security, privacy, and/or confidentiality of information contained in Doyon systems; and investigate and assess the security of our systems more broadly. We are issuing notifications to potentially affected individuals. In response to this event, we are also reviewing and enhancing our information security policies and procedures and have already implemented new security controls to help avoid future incidents.

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 24 months. 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 (ActivationDeadline)>> 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

We recommend that you take the following steps to monitor for any potential misuse of your personal information:

- You should regularly review your account statements and monitor free credit reports.
- Under federal law, you are entitled to obtain one free copy of your credit report every twelve months from each of the nationwide consumer reporting agencies. You can obtain a free copy of your credit report from each agency by calling 1-877-322-8228 or visiting www.annualcreditreport.com. We recommend that you periodically obtain credit reports from each nationwide credit reporting agency. If you discover information on your credit report arising from a fraudulent transaction, you may request that the credit reporting agency delete that information from your credit report file.
- You may also consider contacting the credit reporting agencies directly if you wish to put in place a fraud alert or a security freeze. A fraud alert will notify any merchant checking your credit history that you may be the victim of identity theft and that the merchant should take additional measures to verify the application. Contacting any one of the three agencies will place an alert on your file at all three. A security freeze restricts all creditor access to your account but might also delay any requests you might make for new accounts. You may contact the nationwide credit reporting agencies at the following numbers to place a security freeze to restrict access to your credit report:
    - Equifax: 800-349-9960; www.equifax.com; P.O. Box 740241, Atlanta, GA 30374-0241
    - Experian: 1-888-EXPERIAN (397-3742); www.experian.com; P.O. Box 9554, Allen, TX 75013
    - TransUnion: 888-909-8872; transunion.com; Fraud Victim Assistance, P.O. Box 2000, Chester, PA 19022-2000

  You will need to supply your name, address, date of birth, Social Security number, and other personal information. The agencies are not permitted to charge you for placing or lifting a freeze. Each credit reporting agency will confirm your request with a unique PIN or password that you will need in order to lift or remove the freeze. You should keep the PIN or password in a safe place.
- To report incidents of fraud and identity theft, you can contact the Federal Trade Commission (FTC) at 1-877-ID-THEFT or through their website at https://www.identitytheft.gov/. You can also contact local law enforcement or your state's attorney general.

FOR MORE INFORMATION

If you have questions or concerns about this, or if we can be of further assistance to you, please do not hesitate to call us at 1-866-461-2674, Monday through Friday from 8:00 a.m. to 5:30 p.m. Alaska Time, excluding major U.S. holidays. Please have your membership number ready.

Sincerely,

Sarah E. Obed

Sarah E. Obed
Senior Vice President, External Affairs

IMPORTANT CONTACT INFORMATION

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 obtain information about avoiding identity theft from the FTC. The FTC can be reached at:

Federal Trade Commission
1-877-ID-THEFT (1-877-438-4338)
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20850
consumer.ftc.gov

IF YOU ARE A MARYLAND RESIDENT: You may also obtain information about avoiding identity theft from the Maryland Attorney General's Office. This office can be reached at:

Office of the Attorney General
Consumer Protection Division
200 St. Paul Place
Baltimore, MD 21202
(888) 743-0023
marylandattorneygeneral.gov

IF YOU ARE A NORTH CAROLINA RESIDENT: You may also obtain information about preventing identity theft from the North Carolina Attorney General's Office. This office can be reached at:

North Carolina Department of Justice
Attorney General Roy Cooper
9001 Mail Service Center
Raleigh, NC 27699-9001
(877) 566-7226
ncdoj.com

IF YOU ARE A RHODE ISLAND RESIDENT: This incident affected approximately 10 Rhode Island residents. You may also obtain information about preventing identity theft from the Rhode Island Attorney General's Office. This office can be reached at:

Rhode Island Office of the Attorney General
150 South Main Street
Providence, RI 02903
(401) 274-4400
riag.ri.gov

IF YOU ARE A NEW YORK RESIDENT: You may also obtain information about preventing identity theft from the New York Department of State's Division of Consumer Protection. This office can be reached at:

New York State Division of Consumer Protection
123 William Street
New York, NY 10038-3804
1 (800) 697-1220
www.dos.ny.gov/consumerprotection

One Commerce Plaza
99 Washington Ave.
Albany, NY 12231-0001

IF YOU ARE A DISTRICT OF COLUMBIA RESIDENT: You may also obtain information about preventing identity theft from the D.C. Attorney General's Office. This office can be reached at:

Office of Consumer Protection
441 4th Street, NW
Washington, DC 20001
(202) 442-9828
oag.dc.gov/consumer-protection.

IF YOU ARE A CONNECTICUT RESIDENT: You may also obtain information about preventing identity theft from the Connecticut Attorney General's Office. This office can be reached at:

Office of the Attorney General,
165 Capitol Avenue,
Hartford, CT 06106,
1-860-808-5318
www.ct.gov/ag.

IF YOU ARE A MASSACHUSETTS RESIDENT: You may also obtain information about preventing identity theft from the Massachusetts Attorney General's Office. This office can be reached at:

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.