Kaycan Group of Companies / Le Groupe Kaycan
Attn: Human Resources Director
3075 Trans-Canada Highway
Pointe-Claire QC
H9R 1B4, Canada

29286

March 24, 2023

000001

[redacted]

Re: Notice of Data Security Incident

Dear [redacted]:

We are writing to notify you of a recent data security incident with the Kaycan Group of Companies (Kaycan) that might involve some of your personal information. This letter is being sent to provide you with additional information and to advise you of services Kaycan is offering at no charge to you to help protect your continued privacy.

It is important to note that we have no evidence at this time that your personal information has been used inappropriately or fraudulently, but we are sending this letter to tell you what happened, what information was potentially involved, what we have done and what you can do to address this situation.

What Happened?

We detected suspicious activity on our systems that we have since confirmed to be a data security incident. We immediately launched an investigation and recovery effort with the assistance of cyber experts and law enforcement. Our investigation revealed that an unauthorized third party gained access to Kaycan systems and took certain files that likely contain confidential company and employee information. Our investigation has not yet established exactly when this happened, but we now believe it may have been March 2, 2023.

What Information Was Involved?

Through our investigation, we have learned that information from our human resources system may have been compromised. We are unable to say with certainty what information about which employees or former employees was affected. We are working hard to determine whether your name, address, social security number, payroll information, health benefits data, and passport information were involved. In addition, any personal information that you voluntarily stored or used on any Kaycan computer issued to you may have been compromised. At this time, we do not know with certainty what information was involved, and unfortunately, may never know what specific data has been compromised. We are communicating to you so that you can take the steps outlined below to protect yourself.

What We Are Doing

Immediately upon learning of this incident, we launched an investigation and recovery effort with the assistance of cyber experts and law enforcement. Determining whether information was compromised in any way has been one of the top priorities of this effort so that we could notify potentially affected individuals. Rest assured, we are also working with cybersecurity experts to reinforce our systems and information security protocols in an effort to prevent incidents like this from occurring in the future.

To help protect your identity, we have retained the assistance of Cyberscout, a TransUnion company specializing in fraud assistance and remediation services.

Through Cyberscout, we have arranged for a two-year subscription to an online monitoring service, at no cost to you. This credit monitoring service will notify you by email of critical changes to your Credit Report. Should you receive an email alert, you can review and validate the reported change by logging into the portal. This allows you to identify any potentially fraudulent activity on your Credit Report.

We encourage you to take advantage of this service and help protect your identity. To activate your service, please visit: **https://secure.identityforce.com/benefit/kaycan**

You will be prompted to enter the following activation code: [redacted]

Please ensure that you redeem your activation code before 7/16/2023 to take advantage of the service.

Upon completion of the enrollment process, you will have access to the following features:

- ✓ Access to a credit report with credit score. A credit report is a snapshot of a consumer's financial history and primary tool leveraged for determining credit-related identity theft or fraud.
- ✓ Credit monitoring alerts with email notifications to key changes on a consumer's credit file. In today's virtual world, credit alerts are a powerful tool to protect against identity theft, enable quick action against potentially fraudulent activity, and provide overall confidence to potentially impacted consumers.
- ✓ Dark Web Monitoring to provide monitoring of surface, social, deep, and dark websites for potentially exposed personal, identity and financial information in order to help protect consumers against identity theft.
- ✓ Identity theft insurance of up to $1,000,000 in coverage to protect against potential damages related to identity theft and fraud.[1]
- ✓ Assistance with reading and interpreting credit reports for any possible fraud indicators.
- ✓ Assistance with answering any questions individuals may have about fraud.

Should you have any questions regarding the Cyberscout solution, have difficulty enrolling, or require additional support, please contact Cyberscout at 1-877-694-3367.

What You Can Do

To help protect your personal information, we strongly recommend you take the following steps:

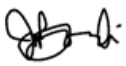
- Enroll in the credit monitoring service that we are offering to you. This will enable you to get alerts about any efforts to use your name and personal information to establish credit and to block that credit from being established if you were not the one who initiated it.
- Carefully review statements sent to you by your bank, credit card company, or other financial institutions as well as government institutions like the Internal Revenue Service (IRS). Notify the sender of these statements immediately by phone and in writing if you detect any suspicious transactions or other activity you do not recognize.
- The attached **Reference Guide** describes additional steps that you can take and provides resources for additional information. We encourage you to read and follow these steps as well.

For More Information

If you have questions or concerns or learn of any suspicious activity that you believe may be related to this incident, please call 1-833-806-1882, Monday through Friday from 9 a.m. – 6:30 p.m. Eastern Standard Time, excluding holidays.

Please know that we take this matter very seriously, and we apologize for the concern and inconvenience this may cause you.

Sincerely,



Joseph N. Bondi
Vice President

REFERENCE GUIDE

In the event that you suspect that you are a victim of identity theft, we encourage you to remain vigilant and consider taking the following steps:

Order Your Free Credit Report. To order your free credit report, visit www.annualcreditreport.com, call toll-free at 877-322-8228, or complete the Annual Credit Report Request Form on the U.S. Federal Trade Commission's website at www.ftc.gov and mail it to Annual Credit Report Request Service, P.O. Box 105281, Atlanta, GA 30348-5281. Do not contact the three credit bureaus individually; they provide your free report only through the website or toll-free number.

When you receive your credit report, review the entire report carefully. Look for any inaccuracies and/or accounts you don't recognize, and notify the credit bureaus as soon as possible in the event there are any.

You have rights under the federal Fair Credit Reporting Act ("FCRA"). These include, among others, the right to know what is in your file; to dispute incomplete or inaccurate information; and to have consumer reporting agencies correct or delete inaccurate, incomplete, or unverifiable information. For more information about the FCRA, please visit https://www.consumer.ftc.gov/articles/pdf-0096-fair-credit-reporting-act.pdf or www.ftc.gov.

Place a Fraud Alert on Your Credit File. To protect yourself from possible identity theft, consider placing a fraud alert on your credit file. A fraud alert helps protect you against the possibility of an identity thief opening new credit accounts in your name. When a merchant checks the credit history of someone applying for credit, the merchant gets a notice that the applicant may be a victim of identity theft. The alert notifies the merchant to take steps to verify the identity of the applicant. You can report potential identity theft to all three of the major credit bureaus by calling any one of the toll-free fraud numbers below. You will reach an automated telephone system that allows you to flag your file with a fraud alert at all three bureaus.

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	1-800-525-6285	www.equifax.com
Experian	P.O. Box 9532 Allen, Texas 75013	1-888-397-3742	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	1-800-680-7289	www.transunion.com

Place a Security Freeze on Your Credit File. You have the right to place a "security freeze" on your credit file. A security freeze generally will prevent creditors from accessing your credit file at the three nationwide credit bureaus without your consent. You can request a security freeze free of charge by contacting the credit bureaus at:

Equifax	P.O. Box 740241 Atlanta, Georgia 30374-0241	www.equifax.com
Experian	P.O. Box 9554 Allen, Texas 75013	www.experian.com
TransUnion	Fraud Victim Assistance Division P.O. Box 2000 Chester, Pennsylvania 19016	www.transunion.com

The credit bureaus may require that you provide proper identification prior to honoring your request. In order to request a security freeze, you will need to provide the following information:

1. Your full name (including middle initial as well as Jr., Sr., II, III, etc.)
2. Social Security number
3. Date of birth
4. If you have moved in the past five (5) years, provide the addresses where you have lived over the prior five years.
5. Proof of current address, such as a current utility bill or telephone bill
6. A legible photocopy of a government issued identification card (state driver's license or ID card, military identification, etc.)
7. If you are a victim of identity theft, include a copy of either the police report, investigative report, or complaint to law enforcement agency concerning identity theft

Placing a security freeze on your credit file may delay, interfere with, or prevent timely approval of any requests you make for credit, loans, employment, housing or other services. For more information regarding credit freezes, please contact the credit reporting agencies directly.

Contact the U.S. Federal Trade Commission. If you detect any incident of identity theft or fraud, promptly report the incident to your local law enforcement authorities, your state Attorney General and the Federal Trade Commission ("FTC"). If you believe you identity has been stolen, the FTC recommends that you take these additional steps.

- Close the accounts that you have confirmed or believe have been tampered with or opened fraudulently. Use the FTC's ID Theft Affidavit (available at www.ftc.gov/idtheft) when you dispute new unauthorized accounts.
- File a local police report. Obtain a copy of the police report and submit it to your creditors and any others that may require proof of the identity theft crime.

You can learn more about how to protect yourself from becoming an identity theft victim (including how to place a fraud alert or security freeze) by contacting the FTC:

Federal Trade Commission
Consumer Response Center
600 Pennsylvania Avenue, NW
Washington, DC 20580
1-877-IDTHEFT (438-4338)
www.ftc.gov/idtheft

For Maryland Residents: You can obtain information from the Maryland Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the Maryland Attorney General at: 200 St. Paul Place, Baltimore, MD 21202, 888-743-0023, www.oag.state.md.us

For Massachusetts Residents: You have a right to request from us a copy of any police report filed in connection with this incident. If you are the victim of identity theft, you also have the right to file a police report and obtain a copy of it. As noted above, you also have the right to place a security freeze on your credit report at no charge.

For New York Residents: You may also contact the following state agencies for information regarding security breach response and identity theft prevention and protection information:

New York Attorney General's Office
Bureau of Internet and Technology
(212) 416-8433
https://ag.ny.gov/internet/resource-center

NYS Department of State's Division of
Consumer Protection
(800) 697-1220
https://www.dos.ny.gov/consumerprotection

For North Carolina Residents: You can obtain information from the Federal Trade Commission and the North Carolina Office of the Attorney General about steps you can take to help prevent identity theft. You can contact the North Carolina Attorney General at: 9001 Mail Service Center, Raleigh, NC 27699, 1-877-566-7226, www.ncdoj.gov

For Oregon Residents: State laws advise you to report any suspected identity theft to law enforcement, as well as the Federal Trade Commission. You can contact the Oregon Attorney General at: Oregon Department of Justice, 1162 Court Street NE, Salem, OR 97301-4096, (877) 877-9392, www.doj.state.or.us.

[1]In the unlikely event that your information is abused, services offered include a personal fraud specialist who will help to resolve any identity fraud issues including working with relevant agencies, business and institutions for the duration of your subscription. Once you have enrolled in TransUnion Cyberscout credit monitoring, should you experience fraud resulting in a financial loss, you will gain access to a $1,000,000 insurance reimbursement policy. The expense reimbursement insurance benefit for members is underwritten by certain Underwriters at Lloyd's, under a master group policy issued in the name of Cyberscout Limited, Sontiq Inc. and all subsidiaries for the benefit of members.