As you are aware, on February 19th, our Company was the subject of a malware attack. We value our employees and we sincerely appreciate how you have worked tirelessly to continue business operations during this challenging period. As we return to ordinary business operations, many of you may be understandably concerned about how the malware attack may have affected your own personal information.

We want to let you know that the Company has retained advisors to assist with an investigation into what occurred. Although the investigation is ongoing, this communication provides you with information about what happened, what data was affected, what we are doing and what you can do to protect yourself.

We also would like to announce that the Company has made arrangements for you to enroll in *myTrueIdentity,* provided by Trans Union, at no cost to you. We purchased this package proactively for our employees benefit and protection, although **at this point we do not have evidence that you are at a risk of harm from this incident**. In the coming days you will receive your enrollment code and instructions. We encourage you to enroll in this program.

WHAT HAPPENED?

Around midnight between February 18 and 19, 2020, the Company was the victim of a malware attack. An intruder into our information technology systems commenced a process that resulted in the encryption of our data. Although the investigation is ongoing, it is likely that the intrusion began at least by February 10, 2020.

WHAT INFORMATION WAS INVOLVED

At this point in the investigation, we do not know what data may have been taken from our systems or whether that information may have included the personal information of our employees. At this time, we do know that employee personal information was affected by the malware which encrypted the data stored on our servers. Some of the data that was encrypted included employee information such as titles, business contact information, personal contact information, dependent and emergency contact information, salary and benefits, and other information that forms part of your personnel file. Payroll data that was stored in Payroll Guardian was not affected unless you copied that data to company systems. However, **please note that the fact that your personal information was affected by the malware does not necessarily mean that it was accessed or taken by the intruder**.

WHAT WE ARE DOING

Since first learning about this illegal intrusion, we have been working to restore our systems, to understand how this happened, and to determine what information and individuals were impacted, as well as to identify what steps that we could take to support our employees and customers.

As a precaution, we have arranged for Trans Union to provide you with a 2-year subscription to TransUnion *myTrueIdentity*, an online credit monitoring service, at no cost to you.

This credit monitoring service will notify you by email of critical changes to your TransUnion Credit Report. Should you receive an email alert, you are able to review and validate the reported change by

logging into our portal. This allows you to identify any potentially fraudulent activity on your TransUnion Credit Report.

In addition, you will have access to identity theft insurance of up to $50,000 to protect against damages related to identity theft and fraud as well as dark web monitoring to look for potentially exposed personal identity and financial information.

An information sheet with instructions from Trans Union and your assigned activation code will be distributed in the coming days by your onsite Human Resources representative.

WHAT YOU CAN DO

1) We hope that you will take advantage of *myTrueIdentity*. The process for signing up requires you to authenticate yourself, so it will take some time to enroll. However, we believe *myTrueIdentity* can be an important part of each of us protecting ourselves from fraud and identity theft from the increasingly pervasive threats in the online world.

2) Please remain vigilant against threats of identity theft or fraud. Regularly review and monitor your account statements and credit history for any signs of unauthorized transactions or activity.

3) Be alert for "phishing" emails by someone who acts like they know you and requests sensitive information over email, such as passwords, your Social Insurance Number, or bank account information. Do not respond to unsolicited offers of technical computer support from people claiming to be from the Company or companies we work with.

4) Do not open attachments or click on links in emails or text messages from senders that you do not know or that you were not expecting. Review email addresses and the names in links to ensure that they have not been modified. It is common for a malicious actor to slightly alter an email address or a website link in the hopes that you will not notice.

For other steps you can take, please see below.

OTHER IMPORTANT INFORMATION.

We regret this incident occurred and any concern this may have caused you. Should you have questions, or if you would like to discuss the matter further, please contact your onsite Human Resources representative.

Sincerely,

OTHER STEPS YOU CAN TAKE

<u>Free Credit Reports</u>

Even if you do not take advantage of *myTrueIdentity*, you are entitled to obtain a free credit report from each of Equifax and TransUnion to review your credit file for signs of fraud or identity theft. We have included contact information for Equifax and TransUnion below.

Equifax:	TransUnion:
Consumer Relation P.O. Box 190, Station JeanTalon Montreal PQ H1S 2Z2	Consumer Relations 3115 Harvester Road, Suite 201 Burlington ON L7L 3N8
1-800-465-7166	1-800-663-9980
www.equifax.ca	www.transunion.ca

Fraud Alerts

You may also consider placing a fraud alert on your credit file that requires businesses to verify your identity before issuing you credit. You may arrange for this service directly through the credit reporting agencies listed above. There is a charge of this service and it can only be made available to you with your express consent.

Report Identity Theft or Fraud

If you suspect that you may have been a victim of identity theft or fraud, you should consider contacting your local police and visit the Canadian Anti-Fraud Centre for support (http://www.antifraudcentre-centreantifraude.ca). You should also review the RCMP's Identity Theft and Identity Fraud Victim Assistance Guide for steps you can take if you are the victim of identity theft or identity fraud. Visit www.rcmp-grc.gc.ca/scams-fraudes/victims-guide-victimes-eng.htm.