Drivers Industrial Installations Ltd.
P.O. Box 149
Freshwater, NL A0B1W0
T: 709.726.6820

May 14, 2021

Privacy Breach Notification

Following issuance of a notification to persons impacted by a recent security incident experienced by a service provider of Drivers Industrial Installations Ltd. involving personal information, we would like to update TradesNL union leadership regarding this matter to assist with communication to affected member personnel.

Attached for your information is a copy of the Notice to Affected Persons that was issued in relation to this situation.

We sincerely regret that this happened and appreciate the impact this may have for affected trade union members. Please rest assured that we are doing everything we can to rectify the situation.

In addition to the information provided in the attached Notice, Drivers Industrial Installations Limited will cover the cost for all affected members to receive credit monitoring for one year upon request. A follow up letter to affected members will be issued next week outlining the process to avail of the credit monitoring.

We also ask that you reinforce the advice provided in the Notice which is designed to mitigate the risks to affected members. This includes the following:

i. Be vigilant against others gathering information by deception.

ii. Request a credit report. At any time, affected members can receive a report from the national credit bureaus:
   - **Equifax**: 1-800-465-7166; www.equifax.ca
   - **TransUnion**: 1-800-663-9980; www.transunion.ca

iii. Place a fraud alert on their credit report.

iv. Continue to monitor their credit reports.

We sincerely regret this privacy breach and assure you steps are being taken to prevent a recurrence.

Should affected members have any questions about this incident, they may call 780-665-6706 during normal business hours. Alternatively, they may email inquiries to: inquiries@nextdigital.xyz.

April ___, 2021

Notification of Privacy Breach

We value the importance of protecting your personal information and take the security and privacy of information in our care seriously. As a result, we are writing to you with important information about a recent security incident involving your personal information.

What happened?

On April 8, 2021, we learned that one of our service providers had been the victim of a sophisticated, illegal ransomware attack which resulted in hackers gaining access to employee files containing personal information.

As soon as our service provider became aware of this incident, it contained the breach by immediately blocking all further access to the network. Our service provider also engaged independent cyber security experts, to provide analysis and monitoring of the network for any ongoing threats and prevent further unauthorized access, to protect our employees, partners and businesses.

What Information Was Involved?

A description of your personal information that may have been accessed as a result of this breach is set out below:

a. full name;
b. date of birth;
c. gender;
d. Social Insurance Number;
b. home address, including postal code;
c. email address;
d. phone number;
d. job title or position;
e. employee code and employment status;
f. banking information; and/or
g. salary information.

What We Are Doing.

As we are committed to continuously improving, we are working to identify and make changes based on lessons learned from this incident. In particular, we are reviewing our privacy policies and procedures. We are also reviewing our agreements with our service providers. As for the service provider who experienced this ransomware attack, we have been advised that:

a. they have engaged third party security experts to provide rapid incident containment, mitigation and recovery assistance;
b. they will continue to monitor their IT systems for potential threats;
c. they have required employees to change their passwords to meet certain security parameters;

d. they are reviewing their current privacy policy and procedures;
e. they are implementing improvements to their security, including multiple factor authentication for system access;
f. they are enhancing their cyber security training for all users of their IT systems; and
g. they have notified the appropriate law enforcement authorities.

What You Can Do?

We would encourage you to be vigilant against third parties attempting to gather information by deception (commonly known as "phishing"), including through links to fake websites.

To the extent applicable, you may also wish to consider the following steps:

- Request a credit report. At any time, you can receive a report from the national credit bureaus:
  - **Equifax**: 1-800-465-7166; www.equifax.ca
  - **TransUnion**: 1-800-663-9980; www.transunion.ca

  Remain vigilant about suspicious activity and check your credit reports, as well as your other account statements periodically. Immediately report any suspicious activity to the credit bureaus. It is commonly recommended practice to request a credit report from time to time.

- Place a fraud alert on your credit report. To place a fraud alert on your credit file, contact Equifax or TransUnion at the numbers provided above. A fraud alert tells creditors to contact you before they open any new credit accounts or change your existing accounts. This can help prevent an identity thief from opening additional accounts in your name. As soon as one of the credit bureaus confirms your fraud alert, the other credit bureau will be automatically notified in order to place alerts on your credit report, and the reports will be sent to you free of charge. When you establish a fraud alert, you will receive a follow-up letter that will explain how you can receive a free copy of your credit report. When you receive your credit report, examine it closely and look for signs of fraud, such as credit accounts that are not yours.

- Continue to monitor your credit reports. Even with a fraud alert on your account, you should continue to monitor your credit reports to ensure that an imposter has not opened an account with your personal information.

Should you have any questions about this incident, you may call 780-665-6706 during normal business hours. Alternatively, you may email inquiries to: inquiries@nextdigital.xyz.