Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	DIRTT Environmental Solutions Ltd. (Organization)
Decision number (file number)	P2018-ND-095 (File #009310)
Date notice received by OIPC	July 27, 2018
Date Organization last provided information	July 27, 2018
Date of decision	August 2, 2018
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those individuals in Alberta pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization operates in Alberta and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The following information was involved in this incident: • name, • address, • social insurance number (SIN), • banking information, • employment information, and • in very limited instances, some health information of past and present employees, board members and senior leadership members. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• In or around August 2017, an unauthorized forwarding rule was installed on the Outlook mailbox of the Organization's internal legal counsel. As a result, copies of all incoming emails were forwarded to an unauthorized third-party Gmail account. The incident was likely the result of a phishing attack. • The investigation revealed that approximately 17,000 emails were transferred over a ten (10) month period. Of those, approximately 800 documents were identified as potentially containing some form of personal identifiable information of approximately 1000 individuals, most of which are current and past employees and board members. • The suspicious email forwarding rule was discovered on May 29, 2018, when the Organization's internal cybersecurity expert was deploying a new cybersecurity defense solution that would proactively detect unusual activity on the Organization's systems.
Affected individuals	The Organization reported there were "Approximately 1000 potentially affected individuals."
Steps taken to reduce risk of harm to individuals	• Disabled all known forwarding rules and changed the password of the email account in question. • Conducted an internal investigation. • Engaged the services of a document review service to determine what personal information was in the 13,000 emails which were forwarded. This included a document by document review. • Retained a cybersecurity forensics firm to investigate the incident, secure the network and mitigate any impacts.
Steps taken to notify individuals of the incident	The Organization reported that it "…intends to notify the affected individuals in the coming days, and can provide a copy of the notification letter to the OIPCA on request".
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	The Organization reported "While [the Organization] is not aware of any attempts to utilize the information, it is possible the information could be used for identity theft, fraud and to the extent some of the information regarding some of the senior leadership members is utilized, reputational harm." I agree with the Organization's assessment of the types of harm that might result from this incident. The contact, identity, financial, employment and, in some cases, health information could be used to cause the significant harms of identity theft, fraud, and reputational damage.

Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	The Organization reported that it "While [the Organization] is not aware of any attempts to utilize the compromised information, given the large amount of information involved, the length of time during which the unauthorized forwarding was in place, and the large number of potentially affected individuals involved, there is a possibility that harm could result." I agree with the Organization's assessment. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and misdirection of email), and the information was exposed for a 10 month period.

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals as a result of this incident.

The contact, identity, financial, employment and, in some cases, health information could be used to cause the significant harms of identity theft, fraud, and reputational damage. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and misdirection of email), and the information was exposed for a 10 month period.

I require the Organization to notify affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) and confirm to my office in writing that it has done so, providing a copy of the notification letter, within 10 days of the date of this decision.

Jill Clayton
Information and Privacy Commissioner