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)	P2021-ND-029 (File #016486)
Date notice received by OIPC	September 10, 2019
Date Organization last provided information	September 10, 2019
Date of decision	February 23, 2021
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 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) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved some or all of the following information: • name, • email address, • employer, • dietary restrictions, • credit card information including CVV code, and • other registration information (e.g. special requests, roommate preferences). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On August 12, 2019, an Excel spreadsheet containing certain personal information was inadvertently emailed to the Organization's internal sales representatives distribution list.

	• The list included mainly internal Organization email addresses; however, there were some external email addresses (for individuals within the Organization's sales network). • The breach was discovered on August 13, 2019 by the employee who sent the email. • On August 13, 2019, an email was sent to those on the original distribution list advising them of the error and requesting they delete the email and, if they had forwarded it, requesting that they ask the recipient to delete the email. • The Organization's IT team also endeavoured to scrub the Organization's network to remove the email from the recipients' inboxes.
Affected individuals	The incident affected individuals 370 individuals, including 43 residents in Alberta.
Steps taken to reduce risk of harm to individuals	• Advised affected individuals of what had happened and recommend steps they could take to protect themselves from the possibility of identity theft or financial loss. • Offered pre-paid one-year subscription for identity theft and credit monitoring to affected individuals. • Reviewing and revising privacy and other applicable policies as necessary. • Considering implementing privacy-sensitivity, data security and other training for its employees.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on August 24, 2019 and by letter on August 30, 2019.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to 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, *With respect to much of the information disclosed, potential harms to affected individuals include financial loss, fraud, and identity theft.* *Email addresses, particularly in combination with other personal information elements, could be used for phishing purposes, increasing vulnerability to identity theft and fraud.* *Finally, the disclosure of dietary restrictions and roommate preferences could potentially cause: (i) embarrassment; (ii) mental harm; and/or (iii) damage to the reputation of the affected individuals.* I agree with the Organization's assessment. A reasonable person would consider that the contact and financial information at issue

	could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the vulnerability to identity theft and fraud. Information about dietary restrictions or roommate preferences could be used to cause hurt, humiliation and embarrassment, as well as damage to relationships. These are all significant harms.
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: *The following factors militate in favour of a low likelihood of harm:* *(i) the Excel spreadsheet was emailed to a limited number of individuals;* *(ii) all of the recipients are known … In particular, the vast majority of the recipients are employees … and all other recipients are individuals with whom [the Organization] has a very close/friendly relationship arising from their business arrangement;* *(iii) [The Organization] trusts each of the recipients with confidential information in the normal course of its operations;* *(iii) [sic] there is no evidence of any malicious intent or purpose by either the sender of the email or any of its recipients;* *(iv) the information was not exposed for a long period. As discussed below, efforts were made… to promptly delete the email from recipients' inboxes;* *(v) [The Organization] promptly sent each of the recipients an email: (i) requesting the deletion of the original email (i.e. containing the Excel spreadsheet); and (ii) reminding them that such information was confidential; and* *(vi) the personal information of no vulnerable persons was included in the spreadsheet.* *An individual's name and mailing addresses are not, by themselves, sensitive information; but credit card information, roommate preferences and dietary restrictions are. As such, the disclosure of such information militates in favour of an increased likelihood of harm.*

	Based on the foregoing, the factors point to a very low likelihood of harm arising from this breach… In my view, a reasonable person would consider that the likelihood of harm resulting from his breach is decreased because it was the result of human error and not malicious intent, and because the unauthorized recipients are known and trusted by the Organization. Nonetheless, it is not clear whether the Organization received confirmation from the unintended recipients that the email was deleted and not copied, forwarded or otherwise distributed. Further, the likelihood of personal/professional relationships between the recipients and the affected individuals increases the risk of hurt, humiliation, embarrassment or damage to relationships in this case.

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.

A reasonable person would consider that the contact and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing the vulnerability to identity theft and fraud. Information about dietary restrictions or roommate preferences could be used to cause hurt, humiliation and embarrassment, as well as damage to relationships. These are all significant harms.

The likelihood of harm resulting from his breach is decreased because it was the result of human error and not malicious intent, and because the unauthorized recipients are known and trusted by the Organization.

Nonetheless, it is not clear whether the Organization received confirmation from the unintended recipients that the email was deleted and not copied, forwarded or otherwise distributed. Further, the likelihood of personal/professional relationships between the recipients and the affected individuals increases the risk of hurt, humiliation, embarrassment or damage to relationships in this case.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals by email on August 24, 2019 and letter on August 30, 2019 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner