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	Direct Energy Marketing Limited (Organization)
Decision number (file number)	P2021-ND-071 (File #018114)
Date notice received by OIPC	November 18, 2020
Date Organization last provided information	February 25, 2021
Date of decision	March 9, 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 whose personal information was collected in Alberta pursuant to section 37.1 of *the Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • user name, • email address, • password, • bank account number, • transit number, and • institution number. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The personal information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On November 3, 2020, the Organization's service provider, Kitewheel LLC., was subject to a ransomware cyberattack. The threat actor accessed and exfiltrated personal information and demanded a ransom payment. • While the data were stored in an encrypted database, it is reported that the threat actor obtained access credentials and was able to de-crypt the records for extraction. • The Organization was notified of the breach on November 3, 2020, and was further notified on November 13, 2020 that the personal information of its customers was affected.
Affected individuals	The incident affected 26,470 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Kitewheel notified the Federal Bureau of Investigation (FBI). • Contained and investigated the incident in cooperation with Kitewheel. • Offered affected individuals an identity protection product. • Reset passwords for affected accounts. • Suspended activity with Kitewheel that involved processing of personal information involved with this breach. • Considering additional steps to prevent a similar even from occurring in the future.
Steps taken to notify individuals of the incident	Affected individuals were notified by email, or by telephone/mail where emails "bounced back," on November 27, 2020.
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 reports: *Fraud or similar harms arising from misuse of login credentials to access unrelated accounts for which passwords may be reused.* *The banking information was name, bank account number, transit / branch number and bank / financial institution number. This information is typically not sufficient to withdraw funds from an individual's account or identity theft.* *Individuals may be at risk of phishing attacks using the information above by hackers who use it to pose as legitimate entities* In my view, a reasonable person would consider the identity, contact, and financial information at issue could be used to cause the harms of identity theft, fraud, and financial loss. Email addresses could be used for the purposes of phishing, increasing

	vulnerability to identity theft and fraud. Credentials (passwords) could be used to compromised other online accounts. These are 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 reports it … *… is not aware of any resulting identity theft, fraud, or financial losses to consumers as of the date of this report.* *The risk of login credentials being misused on other websites will be low, except for users who reused passwords and did not promptly change those reused passwords, and, in any such case, only where password is the only means of authentication (i.e., there is not multi-factor authentication).* *As mentioned above, the risk of identify theft should be low.* *Finally, the risk of phishing attacks appears to be low, based on the fact that [the Organization] has not learned of any attempted phishing attempts as of the date of this report.* In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party who also demanded a ransom payment. The lack of reported incidents to date does not mitigate against future harms, as identity theft and fraud can happen months or even years after a breach. Further, the Organization did not report recovering the records/information at issue, increasing the possibility of harm resulting from this breach.

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 the identity, contact, and financial information at issue could be used to cause the harms of identity theft, fraud, and financial loss. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. Credentials (passwords) could be used to compromised other online accounts. These are significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party who also demanded a ransom payment. The lack of reported incidents to date does not mitigate against future harms, as identity theft and fraud can happen months or even years after a breach. Further, the Organization did not report recovering the records/information at issue, increasing the possibility of harm resulting from this breach.

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, or by telephone/mail where emails "bounced back," on November 27, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner