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)	P2022-ND-057 (File #022872)
Date notice received by OIPC	August 23, 2021
Date Organization last provided information	April 14, 2022
Date of decision	August 30, 2022
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, • date of birth, • contact information (phone number, email address), • account number, • payment history, and • overdue balances. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies. The Organization reported, *"The Fraudster did not have access to payment information, such as credit card information or banking information, driver's license or social insurance number."*
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On July 19, 2021, the Organization learned that an individual located in India was contacting the Organization's customers purporting to be a representative of the Organization (the "Fraudster"). • The Organization discovered that the Fraudster had been provided authorized access to certain customer information by HCL Technologies Limited ("HCL"). • HCL is a contractor that provides customer support services to the Organization. The Fraudster was a customer service agent of HCL located in India who was first provided access to customer information in April of 2021. • The Organization believes the Fraudster was misusing his authorized access to customer information in order to attempt to commit fraud by directing customers to pay invoices using payment information that would result in the diversion of funds. • On July 19, 2021, HCL alerted the Organization and the Fraudster's access to customer accounts was immediately terminated. • The Organization reported that one customer was defrauded. Two other customers were contacted by the Fraudster but not defrauded.
Affected individuals	The incident affected approximately 546 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Reimbursed defrauded customer. • Offered credit monitoring to all 546 customers. • Notified law enforcement in India. • Filed a criminal complaint on or about August 10, 2021. • Immediately revoked the Fraudster's access to personal information and his employment was terminated. • Working with HCL to improve security measures to prevent a similar incident in the future. • Continuing to investigate the incident. • Continuously working to improve and update security measures.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on August 17, 2021, and by regular mail if the emails were returned as not delivered.
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	The Organization reported, *Customers face a risk of fraud, including having their payments diverted from Direct Energy and, potentially, other fraud if the*

also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	*Fraudster is able to impersonate Direct Energy and obtain other personal information from the customers.* In my view, a reasonable person would consider that the contact, identity and account 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 vulnerability to identity theft and fraud. 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, *It is likely that at least some of the customers will be the victims of attempted fraud, but they will not suffer financial harm because they will be reimbursed…* In my view, a reasonable person would consider that the likelihood of identity theft and fraud resulting from this incident is increased because it resulted from deliberate and malicious actions (unauthorized access and theft) by a rogue employee, acting over the course of three (3) months.

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.

The contact, identity and account 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 vulnerability to identity theft and fraud. These are all significant harms.

The likelihood of identity theft and fraud resulting from this incident is increased because it resulted from deliberate and malicious actions (unauthorized access and theft) by a rogue employee, acting over the course of three (3) months.

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 that affected individuals were notified by email on August 17, 2021, and by regular mail if the emails were returned as not delivered. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance