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 and Direct Energy Regulated Services (collectively, Direct Energy, or the Organization)
File number	P2017-ND-27 (File #002009)
Date notice received by OIPC	December 15, 2015
Date Organization last provided information	August 10, 2016
Date of decision	January 31, 2017
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the individuals 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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The following information was involved in this incident: • name, • address, and • account number. 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 and concerns residents of Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On September 2, 2015, the Organization was notified by the Office of the Information and Privacy Commissioner that a complaint had been received concerning the Organization's practices.

	• The Organization initiated an investigation, and discovered that on four separate occasions (January 9, 2015, April 29, 2015, June 5, 2015 and June 12, 2015) communications from one of the Organization's service providers had been emailed to customers in error. In brief, emails addressed to Customer A included an attached letter addressed to Customer B. • The letters were generic in that they were "managed event" mailings; however, they included the personal information at issue.
Affected individuals	The incident affected 1,234 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Notified affected individuals. • Taking steps to contact unintended recipients to request/ confirm that misdirected communications are destroyed/ deleted. • Followed up with service provider to reiterate expectations regarding handling personal information. • Flagged potentially affected accounts for suspicious or unusual activity. • Revised customer verification process. • Monitoring accounts of potentially affected customers. • Changing account numbers of affected customers. • Conducting a root cause analysis to determine how the error occurred and to prevent similar incidents.
Steps taken to notify individuals of the incident	The Organization notified affected individuals in writing on June 21, 2016.
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 that it believes "there to be little to no risk of identity theft or financial loss to the affected individuals" but noted "there may be a risk of unauthorized account access (albeit limited access) and associated mischief (e.g. closing of an account, changing an address, etc.)." I agree with the Organization's assessment. The information at issue does not appear to be particularly sensitive; however, it could be used to access accounts and cause mischief. In certain cases and depending on an individual's circumstances, this could be a significant harm.

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 "in terms of whether a malicious actor could potentially use the disclosed information to cause harm, we believe the likelihood of this occurring is small, given the limited distribution of the information, its non-sensitive nature, and the account protections already in place." In my view, there is a real risk of significant harm resulting from this incident. I recognize that the incident resulted from human error and not malicious intent, there is no personal relationship between the affected individuals and the unintended recipients, and the Organization has now taken steps to flag impacted accounts to prevent unauthorized access. However, I am mindful that in certain cases and depending on an individual's circumstances, the information could be used to cause harm. In particular, I am concerned that there were 4 separate incidents spanning approximately 5 months, and the Organization was not aware of the incidents for approximately 9 months. While there are now additional safeguards in place to protect against unauthorized account access, this was not the case for the 9 months the information was exposed.

DECISION UNDER SECTION 37.1(1) OF PIPA

Given the information reported by the Organization, I have concluded that there is a real risk of harm to the affected individuals in this case. The information at issue does not appear to be particularly sensitive; however, it could be used to access accounts and cause mischief. In certain cases and depending on an individual's circumstances, this could be a significant harm.

I recognize that the incident resulted from human error and not malicious intent, there is no personal relationship between the affected individuals and the unintended recipients, and the Organization has now taken steps to flag impacted accounts to prevent unauthorized access. However, I am mindful that in certain cases and depending on an individual's circumstances, the information could be used to cause harm. In particular, I am concerned that there were 4 separate incidents spanning approximately 5 months, and the Organization was not aware of the incidents for approximately 9 months. While there are now additional safeguards in place to protect against unauthorized account access, this was not the case for the 9 months the information was exposed.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individuals on June 21, 2016 in writing. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner