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	Pengrowth Energy Corporation (Organization)
Decision number (file number)	P2013-ND-29 (File #P2319)
Date notice received by OIPC	April 26, 2013
Date Organization last provided information	July 26, 2013
Date of decision	August 7, 2013
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 is registered to carry on business in Alberta. I have jurisdiction because the Organization is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following personal information from employee share compensation accounts: o name, o address, o password to access online account, o social insurance number, and o compensation information (share portion). In addition to the above, the incident also involved the following information for some individuals: o bank account number and o brokerage account number.

	This information is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On April 12, 2013, an employee reported that shares had been sold from his employee share compensation account without his authorization. • A third party service provider establishes and administers the Organization's employee share compensation accounts. Employees access and manage the accounts via an online site provided by the service provider. • On April 16, 2013, the service provider discovered that eight other employees had also experienced unauthorized sales of shares from their accounts. • The shares were sold on the Toronto Stock Exchange and sale proceeds were directed to bank accounts in Montreal. • The Calgary Police Service was notified of the incident on April 17, 2013. • It is unknown how the incident occurred.
Affected individuals	• Nine Alberta employees of the Organization.
Steps taken to reduce risk of harm to individuals	• The service provider recovered some of the sale proceeds ($230,000 in total) and replaced all shares that were fraudulently sold. • Passwords were reset for all employee accounts. A minimum requirement for password complexity was applied. • The Organization reported the service provider reviewed its system and revised its account access procedures. • The Organization requested the service provider to audit all employee accounts for unauthorized sales or unusual activity in recent months. No further incidents of unauthorized transactions were discovered or reported.
Steps taken to notify individuals of the incident	The nine affected individuals were notified about the incident by telephone on April 17 or 18th, and by email on April 26, 2013. The Organization also notified all employees about the incident and provided information about monitoring share accounts in emails sent April 17-26, 2013.

REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury – that could be caused to those 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 recognized the affected individuals may be at risk for identity theft and fraud. It submitted no financial harm occurred to the affected individuals as all shares fraudulently sold and any proceeds were replaced by the service provider. In my view, the personal information involved is highly sensitive. It involves social insurance numbers and, for some individuals, bank account information. The types of harm that could, and did, result from unauthorized access to the personal information are identity theft and fraud. In my view, 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 acknowledged the nine affected individuals experienced fraud with respect to unauthorized access to their share accounts. It submitted, however, that the other personal information exposed, such as social insurance number, has not been used to commit identity theft to date. The Organization did reset the passwords for the accounts and recognized the risk that the compromised passwords may also be used for other online accounts. In my view, the likelihood of harm resulting from this incident is increased because the personal information was exposed during a fraudulent transaction perpetuated by an individual(s) with nefarious intent. The risk of harm for fraud occurred as a result of this incident.

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 personal information involved sensitive information, such as social insurance numbers, that was exposed during an incident involving fraudulent transactions perpetuated by a person(s) with nefarious intent. These factors contributed significantly to my decision.

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

I understand the Organization notified the nine affected individuals by telephone and in an email dated April 26, 2013, in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner