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	United Farmers of Alberta Co-operative Limited (Organization)
Decision number (file number)	P2017-ND-31 (File #004174)
Date notice received by OIPC	October 28, 2016
Date Organization last provided information	November 29, 2016
Date of decision	February 7, 2017
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is incorporated in Alberta and 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, • telephone number, • account information (payment and purchase histories), • member equity and dividend statements. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On August 16, 2016, the Organization received an email from an individual requesting an email address be linked to a customer account.

	• The Organization approved the request, which allowed the individual to access the account and make the following changes: changed the telephone number, changed the account to "Go Paperless" with information sent to the new email address, order fuel cards (request was denied by the Organization). • On September 30, 2016, the Organization became aware there had been a breach when a customer contacted Customer Service to report he had not received his monthly account statement. • Upon investigating, the Organization discovered the changes made to the account were not authorized. The customer advised that his residence had been broken into in August 2016, which incident may be related to the unauthorized changes to the account.
Affected individuals	The incident affected one (1) resident of Alberta.
Steps taken to reduce risk of harm to individuals	• Cancelled online access to the account. • Notified Customer Finance and Cardlock departments. • Closed the affected account and opened a new one. • Encouraged the affected individual to contact credit agencies. • Notified law enforcement. • Reviewed and confirmed procedures to access accounts with staff involved in the incident.
Steps taken to notify individuals of the incident	The Organization notified the affected individual verbally on discovery of the incident and by letter on November 1, 2016.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 the information at issue could be used to cause "Financial fraud and loss" and "Identity theft and fraud". I agree with the Organization's assessment. The financial profile information at issue could be used to cause identity theft, fraud and financial loss. 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 reported that "Due to the sensitivity of the information involved, the nature of harm stated above is high; however, the risk of harm is low." The Organization explained that "accounts can only be used to make purchases at [the Organization's] locations. Upon discovery of the breach, the [online account] access was removed from the account. The applicable internal departments were notified. The impacted account was closed to prevent any purchases from being made."

	In my view there is a real risk of significant harm in this case. The incident resulted from malicious intent (deliberate unauthorized action) and changes were in fact made to the customer's account. The information was exposed for approximately 1½ months and the Organization was not aware of the incident until notified by the customer. I acknowledge the steps the Organization has taken to prevent any further unauthorized activities on the account; however, this does not necessarily mitigate the potential harm that may result if the financial profile information at issue is used for identity theft or to commit other forms of fraud in other situations.

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 individual. The financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. The incident resulted from malicious intent (deliberate unauthorized action) and changes were in fact made to the customer's account. The information was exposed for approximately 1½ months and the Organization was not aware of the incident until notified by the customer. I acknowledge the steps the Organization has taken to prevent any further unauthorized activities on the account; however, this does not necessarily mitigate the potential harm that may result if the financial profile information at issue is used for identity theft or to commit other forms of fraud in other situations.

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

I understand the Organization notified the affected individual verbally on discovery of the incident and by letter on November 1, 2016. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner