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	Beaumont Credit Union Ltd. (Organization)
Decision number (file number)	P2018-ND-100 (File #009345)
Date notice received by OIPC	July 30, 2018
Date Organization last provided information	July 30, 2018
Date of decision	August 7, 2018
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 operates 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 incident involved all or some of the following information: • first and last name, • account information (number, type, balance, history, account statements), • transaction history, • bill payees and associated account numbers (including 2 third party credit card providers), and • e-transfer details. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On July 17, 2018, fraudulent impersonators contacted the Organization via telephone to obtain access to the on-line banking of a credit union member. • The contact center agent failed to engage adequate safeguards to verify the identity of the caller. The agent assisted the caller in changing passwords and granting access to the member's on-line banking portal. • The perpetrator attempted to fraudulently transfer funds on three occasions. The first occasion was successful and a transfer was completed. The subsequent attempts were blocked by loss detection systems and did not occur. • The breach was discovered on July 18, 2018 via on-going monitoring of unusual transactions via automated systems and an attempt by the perpetrator to send fraudulent e-transfers.
Affected individuals	The incident affected one (1) individual.
Steps taken to reduce risk of harm to individuals	• Changed on-line banking passwords and account numbers. • Placed fraud alerts on the member's credit file and arranged for credit monitoring at the Organization's cost. • Arranged to monitor accounts for any potential unusual activity. • Reimbursed the member for any financial loss suffered. • Provided a refresher seminar to all contact center individuals to remind of best practices in identifying individuals in similar telephone interactions. • Will report the incident to law enforcement.
Steps taken to notify individuals of the incident	The affected individual was notified by telephone and in person on July 18, 19, 23 and 24.
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 "There is potential of financial loss and identity theft as a result of the incident. …There is further fraud risk associated with accounts with other institutions (i.e. bill payees)". I agree with the Organization's assessment. The financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss.

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 "The harm is considered significant because the breach was a result of a deliberate and fraudulent attempt to access funds of the member and the perpetrator was successful in one case." I agree with the Organization. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion and successful fraud). The information was accessed and may be used by the perpetrator to compromise accounts with other institutions.

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 likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion and successful fraud). The information was accessed and may be used by the perpetrator to compromise accounts with other institutions.

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

I understand the affected individual was notified by telephone and in person on July 18, 19, 23 and 24, 2018. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner