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	Omista Credit Union Limited (Organization)
Decision number (file number)	P2020-ND-011 (File #013731)
Date notice received by OIPC	October 18, 2019
Date Organization last provided information	October 18, 2019
Date of decision	February 12, 2020
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 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 based in Moncton, New Brunswick and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The information at issue includes: • name, • social insurance number, • account number (e.g., credit union number, other account information), • date of birth, • address, • telephone number, • email address, or • a combination of the above. 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.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On May 29, 2019, the Organization was made aware of an email phishing incident that affected a number of its employees. In particular, an employee mistakenly clicked on a malicious link after receiving a phishing email, which resulted in unauthorized access to the employee's email account by an unknown third party or parties. • As a result, unauthorized access to personal information belonging to the Organization's members and non-members, which was stored in the employee's email account, may have occurred. • The identity of the third party or parties that accessed the email account without authorization is not known. The Organization reported that "No evidence was found indicating that data was accessed, copied, and/or removed". • The breach was discovered the same day when the Organization's IT team was notified by employees who received the original phishing emails.
Affected individuals	The incident affected 560 individuals, including 3 located in Alberta.
Steps taken to reduce risk of harm to individuals	• Reset passwords for all employees. • Continuing to assess current cybersecurity training and education programs/resources. • Enhancing security, including a new password policy, multi-factor authentication, updated security settings, external vulnerability scans and end-point security and protection measures. • Offering credit monitoring services to all affected parties.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail, telephone and email on August 21, 2019.
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 "The possible harms that may occur as a result of the breach are identity theft and fraud". The Organization also said that it is "Communicating with …members immediately following the incident to remind them to use best judgment when opening email correspondence and warning about the threat of email phishing attacks…". In my view, a reasonable person would consider that the contact, identity, and financial information at issue could be used to cause the significant harms of identity theft and fraud. Email address could be used for phishing purposes, increasing vulnerability to identity theft and fraud.

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: *The types of personal information involved in the breach … when combined and/or when considered with the circumstances of the breach (i.e., malicious threat actor engaging in a phishing attack), involve sensitive personal information.* *Given the type of incident in question (i.e., phishing attack), the involvement of a malicious threat actor, and the sensitivity of the personal information involved, the risk of identity theft or fraud is elevated.* I agree with the Organization's assessment. A reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate action, phishing). Although the Organization reported that "No evidence was found indicating that data was accessed, copied, and/or removed", it did not confirm what evidence it reviewed (e.g. audit logs) that would suggest there is no real risk.

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.

A reasonable person would consider that the contact, identity, and financial information at issue could be used to cause the significant harms of identity theft and fraud. Email address could be used for phishing purposes, increasing vulnerability to identity theft and fraud. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate action, phishing). Although the Organization reported that "No evidence was found indicating that data was accessed, copied, and/or removed", it did not confirm what evidence it reviewed (e.g. audit logs) that would suggest there is no real risk.

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 individuals were notified by mail, telephone and email on August 21, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner