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	Meridian Credit Union (Organization)
Decision number (file number)	P2018-ND-059 (File #007243)
Date notice received by OIPC	December 4, 2017
Date Organization last provided information	January 10, 2018
Date of decision	June 15, 2018
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 an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • email address, • telephone number, • membership number, • account number(s) and, • credit card number(s). 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 via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On November 14, 2017, the Organization learned that an unauthorized individual accessed personal information of members and employees who entered various types of personal information into certain forms on the Organization's public website (e.g. Contact forms, Contest Entry forms, Registration forms). • The Organization's public website is separate from the Organization's online banking platform. The information on the public website was kept on a different platform. • The Organization determined that the unauthorized third party accessed the personal information through a webpage code vulnerability.
Affected individuals	The incident affected 8 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Retained an expert third party to determine if the intrusion was ongoing, the earliest date of compromise and the method of intrusion, the scope of the intrusion, the extent of the data exposure and exfiltration, and provide intelligence about the attacker. • Took the website offline. • Scrubbed the database of all customer data. • Advised all affected individuals (members and employees).
Steps taken to notify individuals of the incident	Affected individuals were notified by email on December 8, 2017.
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 did not specifically identify any harm that might result from this incident, but its notification to affected individuals stated "We encourage you to regularly review your financial statements for any suspicious activity and to be vigilant about suspicious emails that may seek information, particularly any messages that appear to be from (the Organization)". In my view, the financial information at issue (credit card numbers) could be used to cause the significant harms of identity theft, financial loss and fraud. The contact information at issue, as well as email address, could be used for unsolicited telephone calls, emails and phishing. I have previously found phishing to 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 did not specifically provide an assessment of the likelihood that significant harm would result from this incident. In my view, 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). Further, the information may have been exposed for approximately one month.

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.

In my view, the financial information at issue (credit card numbers) could be used to cause the significant harms of identity theft, financial loss and fraud. The contact information at issue, as well as email address, could be used for unsolicited telephone calls, emails and phishing. I have previously found phishing to be a significant harm. 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). Further, the information may have been exposed for approximately one month.

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

I understand the Organization notified affected individuals in an email dated December 8, 2017, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner