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	The Globe and Mail Inc. (Organization)
Decision number (file number)	P2021-ND-100 (File #013429)
Date notice received by OIPC	June 20, 2019
Date Organization last provided information	June 20, 2019
Date of decision	March 31, 2021
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 an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident may have involved some or all of the following information: • first and last name, • username and password, and • credit card information (i.e. credit card number, expiry date and CVV code). 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	• At the end of March 2019, the Organization was contacted by two subscribers (resident outside Alberta) reporting possible fraudulent credit card activity, shortly after the subscribers spoke with a customer service representative (CSR) employed by a third party service provider to the Organization.

	• The Organization investigated, and found that a CSR had used a subscriber's credit card information (which had been collected for legitimate purposes) for an unauthorized personal purpose. • The Organization reviewed all available web logs for all CSRs over the previous year in order to identify any other unauthorized use of personal information. The investigation found suspicious activity with respect to three CSRs over a period of approximately 3 months between January and March 2019. • The investigation did not conclusively determine that personal information was used by these CSRs in an unauthorized manner, but 8 subscribers resident in Alberta provided their payment card data to one of these CSRs during this time period.
Affected individuals	The incident affected 8 individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Engaged a third-party forensic firm to investigate. • Contacted the third party service provider to ensure the CSRs no longer had access to subscriber data. • Enhanced security settings for CSR workstations, including further limiting web access by CSRs.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter in June 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 did not specifically identify potential harm(s) that might result from this incident, but its notice to affected individuals said "...we recommend that you remain vigilant in regularly reviewing and monitoring your account statements. Be alert to any requests for personal information, in particular financial information, account numbers or passwords". In my view, a reasonable person would consider that the contact, credentials, and financial information at issue could be used to cause the harms of identity theft and fraud, or to compromise other online accounts. 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	The Organization did not specifically report its assessment of the likelihood of harm resulting from this breach, but did report that it "...does not have evidence that personal information of the eight customers was used in an unauthorized manner". In my view, a reasonable person would consider that the likelihood of harm resulting in this case is increased because the incident

between the incident and the possible harm.	appears to be the result of malicious intent (rogue employees, possible fraud). The information may have been exposed over the course of three months. The lack of reported incidents of fraud to date does not mitigate against this happening in the future.

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, credentials, and financial information at issue could be used to cause the harms of identity theft and fraud, or to compromise other online accounts. These are significant harms.

The likelihood of harm resulting in this case is increased because the incident appears to be the result of malicious intent (rogue employees, possible fraud). The information may have been exposed over the course of three months. The lack of reported incidents of fraud to date does not mitigate against this happening in the future.

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 the affected individuals were notified by letter in June 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner