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	1873349 Ontario, Inc. (Organization)
Decision number (file number)	P2019-ND-118 (File #010980)
Date notice received by OIPC	December 3, 2018
Date Organization last provided information	December 3, 2018
Date of decision	August 1, 2019
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 involved the following information: • first and last name, • payment card number, expiry date, and security code. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta via the Organization's website, www.1800Flowers.ca, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization received information from a third party indicating that common point of purchase data suggested a potential issue with its website, www.1800Flowers.ca. • On October 30, 2018, the Organization's investigation identified unauthorized access to payment card data from cards used to make purchases on the website from August 15, 2014 to September 15, 2018.

	• The Organization reported the breach occurred June 1, 2016 and ended September 15, 2018.
Affected individuals	The incident affected 7,902 individuals.
Steps taken to reduce risk of harm to individuals	• Disabled website. • Alerted the FBI. • Engaged a computer security firm to conduct an investigation. • Notified customers and encouraged them to review their payment card statements and report any unauthorized charges. • Notified the card brands of the incident and provided a list of card numbers that may have been involved in the incident. • Redesigned website and implemented additional security measures.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail on November 30, 2018.
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 is the potential for fraudulent charges being made using the customer's payment card information." In my view, a reasonable person would consider that the financial information at issue could be used to cause the significant harms of 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 likelihood that harm will result is neutral. Upon learning of the incident, [the Organization] immediately disabled the website, contacted the FBI, and engaged a leading computer sercurity [sic] firm to conduct an investigation. On November 30, 2018, [the Organization] sent notice to involved customers and encouraged them to review their payment card statements and report unauthorized charges. [The Organization] also notified the card brands of the incident and provided a list of card numbers that may have been inolved [sic] to support the payment card networks' efforts to address possible fraud. In many cases, payment card rules limit or eliminate liabilty [sic] for fraudulent chanrges [sic] that are timely reported by cardholders.

	In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach appears to be the result of a deliberate, unauthorized intrusion. The information was exposed for over two years. The Organization can only speculate that individuals will not be held responsible for fraudulent charges.

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 financial information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased as the breach appears to be the result of a deliberate, unauthorized intrusion. The information was exposed for over two years. The Organization can only speculate that individuals will not be held responsible for fraudulent charges.

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 that affected individuals were notified by mail on November 30, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner