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	R.C. Purdy Chocolates Ltd. (Organization)
Decision number (file number)	P2018-ND-081 (File #005038)
Date notice received by OIPC	February 23, 2017
Date Organization last provided information	March 1, 2017
Date of decision	July 16, 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 in Alberta 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 following information was potentially involved: • name, • billing address, • credit card holder name, number and expiry date, and • order delivery address. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Some information was collected in Alberta via the Organization's ecommerce website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization uses a third party service provider, Aptos, Inc. (Aptos), to provide e-commerce services enabling the Organization's customers to order and purchase goods using an internet website.

	• The Organization was informed of the breach in a letter dated February 7, 2017, from its service provider Aptos. • Aptos reported to the Organization that it became aware of anomalous activity on its systems on or about November 28, 2016. Aptos investigated and found that the intrusion began in approximately February 2016 and ended in December 2016 (the Organization has used Aptos as a service provider since May 2016). • Aptos reported the matter to the FBI Cyber Division and the U.S. Department of Justice. Aptos informed the Organization that the U.S. Department of Justice requested that Aptos delay notifying its clients about the potential data breach for at least 60 days.
Affected individuals	A total of 13,627 cardholder accounts were affected, including 2,028 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Aptos reported the matter to the FBI Cyber Division and the U.S. Department of Justice. • Aptos reported to the Organization that it worked with law enforcement to identify the number of affected card holders. • The Organization notified its payment system processor and reported its understanding that card issuers were notified. The Organization understands that card issuers and processors have taken steps to monitor and mitigate fraudulent use of the card accounts exposed. • Reported the incident to the Office of the Information and Privacy Commissioner for British Columbia and to the Privacy Commissioner in Ontario.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on March 1, 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 reported its assessment that: "there is little or no potential for harm to any public institution, body or organization; there is little potential harm to the payment system as a whole; nor any realistic potential to cause a loss of trust of any particular organization in a larger societal sense; nor any real potential risk of physical harm, security, reputational or relationship harm to the [Organization's] customers whose payment and ordering information was exposed during the data breach." Further, "In [the Organization's] current estimation, any risk of credit card fraud is better mitigated by the card issuers and payment system operators, and by law enforcement, all of whom are engaged."

	In my view, the contact and financial information involved (payment card number and expiry date) 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: *Based on the information provided by APTOS, it appears that the breach has been contained and the technical aspects of mitigation have been completed by the service provider.* *Law enforcement has been notified…* *[The Organization's] payment service provider and card issuers have been notified and [the Organization] understands that they are engaging in appropriate protective measures…* *[The Organization] has been informed by APTOS that, to the date of very recent email reports, no fraudulent activity has been detected.* *The unauthorized actors have not yet been identified. There is no reason to suspect that those actors were specifically targeting [the Organization or the Organization's] customers, in particular since APTOS has advised the data breach exposed approximately 40 of APTOS' digital commerce customers.* In my view, the likelihood of harm resulting from this incident is increased because the incident was the result of malicious intent (deliberate intrusion and installation of malware). While the perpetrators may not have been targeting the Organization's customers, it appears that personal information generally was the target of the intrusion. The fact that no fraudulent activity had been detected at the time the breach became known to the Organization does not mitigate against possible future fraudulent uses of the information, particularly considering the information was exposed for approximately 6 months before Aptos became aware of the breach.
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.	

The contact and financial information involved (payment card number and expiry date) could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting is increased because the incident was the result of malicious intent (deliberate intrusion and installation of malware). While the perpetrators may not have been targeting the Organization's customers, it appears that personal information generally was the target of the intrusion. The fact that no fraudulent activity had been detected at the time the breach became known to the Organization does not mitigate against possible future fraudulent uses of the information, particularly considering the information was exposed for approximately 6 months before Aptos became aware of the breach.

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 the affected individuals in a letter dated March 1, 2017, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner