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	Affy Tapple, LLC operating as Mrs. Prindables (Organization)
Decision number (file number)	P2018-ND-080 (File #005076)
Date notice received by OIPC	March 1, 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 the affected individual 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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident may have involved the following information: • first and last name, • email address, • address, • telephone number, • payment card number and expiry date. This information is about identifiable individuals, including one resident of Alberta, and is "personal information" as defined in section 1(1)(k) of PIPA. The information collected in Alberta was associated with a transaction made through the Organization's website www.mrsprindables.com.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization uses a third-party company, Aptos, Inc. (Aptos), to operate and maintain the technology for website and telephone orders. Aptos provides a digital commerce platform that functions as the back-end for the Organization's online store, as well as its order management system. • On February 6, 2017, Aptos advised the Organization that unauthorized person(s) electronically accessed and placed malware on Aptos' platform holding payment card transaction information for about 40 online retailers. • According to Aptos, the incident began in February 2016 and ended in December 2016. • Aptos itself learned of the event in November 2016, but was asked by law enforcement investigating the incident to delay notification to allow the investigation to move forward.
Affected individuals	The incident affected one (1) individual residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Aptos advised the Organization that it worked with a leading cybersecurity firm to remove the malware responsible for this incident, made security updates, strengthened access controls, and is monitoring its systems to further safeguard customer information. • Aptos advised the Organization that it contacted and offered its cooperation to federal law enforcement. • The Organization offered one year of free credit monitoring services to affected customers.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter March 3, 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 stated that "Due to the information potentially exposed, harm is not expected. [The Organization] is unaware of any reports of misuse of the data at issue and we are continuing our investigation of this matter. Aptos has advised us that CVV, security and access codes were not accessed. Aptos also advised us that for some credit cards, at the time of the incident, the expiration date for the card had expired." 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. Email address could be used for phishing purposes, which I have previously found 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 reported that it was informed by Aptos that its "customers make up less than 1% of the total population of potentially impacted customers" and that it "…is unaware of any reports of misuse of the data at issue and we are continuing our investigation of this matter." 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), and the information was exposed for almost one year.

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. Email address could be used for phishing purposes, which I have previously found to be a significant harm. 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), and the information was exposed for almost one year.

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

I understand the Organization notified the affected individual by letter sent March 3, 2017. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner