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	Stampin' Up! (Organization)
Decision number (file number)	P2021-ND-316 (File #021416)
Date notice received by OIPC	June 1, 2021
Date Organization last provided information	June 1, 2021
Date of decision	March 7, 2022
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 headquartered in Utah, USA, and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved some or all of the following information: • name, and • credit card information (card number, expiry date). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information at issue was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On April 14, 2021, the Organization discovered that its ecommerce website, www.paperpumpkin.com, was modified with malicious code, which captured payment card data as it was entered on the website in connection with a purchase. • The Organization investigated and determined that the payment card information that may have been accessed was related to transactions made between June 12, 2020 and November 17, 2020.

	• A limited number of customers reported fraudulent charges on their credit cards.
Affected individuals	The incident affected 4,755 Individuals, including 82 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Notified affected individuals and advised them to report any suspicious activity to their card brand. • Patched the vulnerability and removed the malicious code. • Migrating to a hosted environment that will remove the payment process from its system entirely.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on May 14, 2021.
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 *"Credit card fraud is possible, but card brands are aware of the incident and are likely cancelling compromised cards. Affected individuals have been notified and advised to watch for fraudulent activity and to report anything suspicious promptly so it can been credited by their card brand."* In my view, a reasonable person would consider that the contact and financial information at issue could be used to cause the harms of identity theft and fraud. 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 between the incident and the possible harm.	The Organization reported: *The likelihood of actual harm is low. The fraudulent activity occurred some time ago and card brands are likely cancelling and reissuing compromised cards. Further, it is the policy of card brands to reimburse (sic) fraudulent charges, so impacted individuals should not be responsible for any fraudulent activity that does occur. Impacted individuals have been advised to watch for and report and [sic] suspicious accout (sic) activity.* In my view, a reasonable person would consider 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). The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud. Further, the information may have been exposed for approximately five (5) months.

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 and financial information at issue could be used to cause the harms of identity theft and fraud. These are significant harms. 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). The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud. Further, the information may have been exposed for approximately five (5) months. I require the Organization to notify the affected individuals whose information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified affected individuals by letter on May 14, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner