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	Minted LLC (Organization)
Decision number (file number)	P2020-ND-166 (File #015918)
Date notice received by OIPC	May 28, 2020
Date Organization last provided information	November 2, 2020
Date of decision	December 1, 2020
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 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 all or some of the following information: • name, • login credentials (email address and hashed password), • telephone number, • billing address, • shipping address, • date of birth (fewer than 1 % of affected users), and • wedding anniversary date (fewer than 1 % of affected users). <u>Subset of individuals</u> • name, and • full or partial postal 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	• The Organization became aware of a report that mentioned it as one of ten companies impacted by a potential cybersecurity incident. • On May 15, 2020, the Organization discovered that on May 6, 2020, an unauthorized actor gained access and obtained information from the Organization's user account database.
Affected individuals	The incident affected 12,150 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Notified the U.S federal law enforcement authorities. • Reviewing security protocols and took steps to enhance security. • Continuing investigation and intends to implement additional security enhancements as appropriate. • Informed individuals how to change their password. • Informed individuals to be cautious of any unsolicited communication and avoid clicking on links or downloading attachments from suspicious emails. • Informed individuals to monitor accounts and any credit reports for signs of suspicious activity. • Informed individuals on how to obtain a free credit report and how to place a fraud alert on a credit file. • Informed individuals to contact local law enforcement agency if there is an incident of identity theft or fraud. • Provided individuals with a toll-free hotline for more information about the incident.
Steps taken to notify individuals of the incident	The Organization notified 9,850 affected individuals by direct email from May 28, 2020 through June 1, 2020. The Organization also posted a notice of the incident on its website and on major social media platforms from May 28, 2020 through August 17, 2020. The Organization reported, "Indirect notification is appropriate, because at minimum, the company does not have sufficient contact information to provide direct notice to all affect individuals". The Organization also reported that for this subset of individuals, it "believes that the incident does not give rise to a real risk of significant harm to these individuals."

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 that, for a subset of individuals, *...the affected data for this group consisted of a name and, if provided, a full or partial postal address. Without an email address, the attackers would have no ability to conduct a phishing attack on such individuals, and the information would otherwise not provide attackers with the means to harm such impacted individuals. Given the non-sensitive nature of the affected data for this group (including the lack of an email address), the Company believes that the incident does not give rise to a real risk of significant harm to these individuals.* I accept the Organization's assessment for this subset of individuals. A reasonable person would consider that the information at issue could not be used to cause significant harm to these individuals. The Organization's report to my office did not provide an assessment of the likelihood that the harm will occur to those individuals that had more personal information affected by this incident, but its notification to affected individuals informed the individuals how to change their passwords: *As always, please be cautious of any unsolicited communications that ask you to provided your personal information electronically and avoid clicking or downloading attachments from suspicious emails...It is good practice to monitor your accounts and any credit reports you receive for any signs of suspicious activity.* In my view, a reasonable person would consider the contact and identity information at issue could be used to cause the harms of identity theft, and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all 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, that for a subset of individuals, "the Company believes that the incident does not give rise to a real risk of significant harm to these individuals." I agree with the Organization's assessment of harm for those individuals whose name and full or partial postal codes were the only information affected by the incident. I have already said that the name and postal code only cannot be used to cause significant harm.

	The Organization did not specifically assess the likelihood that significant harm would result from this incident for those individuals who had additional information at issue. In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of unauthorized actors (deliberate intrusion). In addition the Organization reported that the perpetrators obtained (stole) information as a result of the incident information.

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 the contact and identity information at issue could be used to cause the harms of identity theft, and fraud. Email addresses could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of unauthorized actors (deliberate intrusion). In addition the Organization reported that the perpetrators obtained (stole) information as a result of the incident information.

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 Organization notified affected individuals by direct email from May 28, 2020 through June 1, 2020, in accordance with the Regulation. The Organization is not required to notify these affected individuals again.

The Organization is not required to notify the affected individuals whose name and full or partial postal codes were the only information affected by the incident.

Jill Clayton
Information and Privacy Commissioner