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	Trusted Tours & Attractions, LLC (Organization)
Decision number (file number)	P2019-ND-185 (File #013642)
Date notice received by OIPC	July 30, 2019
Date Organization last provided information	July 30, 2019
Date of decision	December 13, 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"	Information involved in the breach included: • name, • billing address, • telephone number, • email address, • payment card type, number, expiry date and security codes). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected via the Organization's website, trustedtours.com.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On June 25, 2019, the Organization investigated after being alerted to potential fraudulent activity occurring on payment cards that were used on its website, trustedtours.com.

	• The investigation found that an unauthorized person added unauthorized code on the website so that payment card information entered by purchasers was copied and sent to an external location. • The unauthorized code was present and active on the site between March 24, 2019 and June 27, 2019.
Affected individuals	The incident affected 50,743 individuals, including 193 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Immediately removed the code and investigated. • Notified payment card brands. • Established a dedicated call center. • Strengthening the security of the website and moving to a check-out method with enhanced security features.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on July 29, 2019.
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 "Stolen payment card information can be used to make fraudulent purchases". I agree with the Organization's assessment. 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. Email addresses could be used for phishing purposes, increasing vulnerability to 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 "Because the payment card network rules generally provide that cardholders are not responsible for unauthorized charges, if reported timely, there is not a significant likelihood that harm will result. To further diminish the likelihood of harm, [the Organization] is recommending that the individuals closely review their payment card statements for any unauthorized charges." In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate action, malicious code and exfiltration). The information appears to have been exposed for over 3 months. The Organization can only speculate that affected individuals will not be held responsible for unauthorized charges. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

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. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are significant harms. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate action, malicious code and exfiltration). The information appears to have been exposed for over 3 months. The Organization can only speculate that affected individuals will not be held responsible for unauthorized charges. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud. 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 affected individuals were notified by letter on July 29, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner