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	Tickets.Expert LLC (Organization)
Decision number (file number)	P2019-ND-082 (File #010109)
Date notice received by OIPC	October 22, 2018
Date Organization last provided information	May 17, 2019
Date of decision	June 24, 2019
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual 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 the following information: • name, • credit/debit card number, expiry date, security codes, and • username and password. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies. The affected individual entered his/her information into the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On September 26, 2018, the Organization was informed by its vendor that provides an add-on to websites (Shopper Approved), that the computer code Shopper Approved uses to facilitate customer reviews had been compromised.

	• The vulnerability was patched and malicious code was immediately replaced, but there was a short period of time of potential exposure of personal information. • The security problem was noticed by the vendor on September 15, 2018 and fixed on September 17, 2018. • The Organization does not know how the vendor discovered the security incident.
Affected individuals	The incident affected 259 individuals, including one in Alberta.
Steps taken to reduce risk of harm to individuals	• Patched the vulnerability and replaced the malicious code with secure code. • Sent breach notification letter to affected individuals recommending to monitor credit and bank statements. • Reviewing its vendors' security protocols to ensure adequate controls are in place. • Requiring vendors to conduct additional penetration testing. • Reviewing its policy and procedures. • Working to integrate additional application security testing into the software development cycle. • Evaluating other security detection and prevention providers.
Steps taken to notify individuals of the incident	The affected individual was notified by letter on October 9, 2018.
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 did not report any specific harms that might result from this incident; however, its notification to affected individuals said "We suggest you contact the issuer of the credit card or bank card information you entered on our website and ask that they cancel the card." In my view, a reasonable person would consider that the financial information and credentials at issue 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 that it is "Uncertain of whether the information was accessed or taken by an unauthorized individual. We are only able to determine who made a purchase or accessed the site during the period of vulernability [sic]". In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased as the breach resulted from malicious intent (malicious code). The information

	may have been exposed for two days. The Organization cannot rule out the possibility that an unauthorized third party accessed, read, copied, or downloaded the personal 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 individual.

A reasonable person would consider that the financial information and credentials at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased as the breach resulted from malicious intent (malicious code). The information may have been exposed for two days. The Organization cannot rule out the possibility that an unauthorized third party accessed, read, copied, or downloaded the personal information.

I require the Organization to notify the affected individual 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 the affected individual in a letter dated October 9, 2018 in accordance with the *Regulation*. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner