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	Bulletproof 360, Inc. (Organization)
Decision number (file number)	P2017-ND-86 (File #005269)
Date notice received by OIPC	March 22, 2017
Date Organization last provided information	June 6, 2017
Date of decision	June 20, 2017
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 pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is based in the state of Washington and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • payment card number, expiration date and security code. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected from Albertans via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On February 23, 2017, the Organization noticed unusual activity relating to customer online transactions. • The Organization investigated and found that an unknown third party had compromised its e-commerce system, potentially affecting customer payment card information.

	• The incident may have affected online transactions on the Organization's e-commerce website from October 26, 2016 to January 31, 2017.
Affected individuals	The incident affected 28,197 individuals, including 170 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Immediately took prompt action to address and stop the activity. • Engaged a computer security firm to examine its systems for any signs of an issue, to review and enhance its systems. • Notified local law enforcement. • Will reimburse any such reasonable, documented costs that the affected individuals' financial institutions decline to pay.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail on March 21, 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.	In its report of the incident, the Organization identified that affected individuals could be at a risk for "financial loss". In my view, the financial information at issue (including payment card numbers, security codes and expiry dates) could be used to cause the significant harms of financial loss, fraud and identity theft.
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.	In its report of the incident, the Organization said the harm is not significant and "The risk for financial loss is low because those affected have been advised to report any unauthorized charges to their financial institution because the major credit card companies have rules that restrict them from requiring cardholders to pay for fraudulent charges that are reported in a timely manner." In my view, 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 on the Organization's website). Further, the information may have been exposed for approximately three months. 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.

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 financial information at issue (including payment card numbers, security codes and expiry dates) could be used to cause the significant harms of financial loss, fraud and identity theft. 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 on the Organization's website). Further, the information may have been exposed for approximately three months. 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. I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified affected individuals by mail dated March 21, 2017 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner