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-162 (File #007191)
Date notice received by OIPC	November 27, 2017
Date Organization last provided information	November 27, 2017
Date of decision	December 8, 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 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 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, • address, • email address, and • 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 residents of Alberta via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization previously notified customers that an unknown third party compromised the Organization's e-commerce website and may have been able to access customer payment card information during the period from October 26, 2016 to May 30, 2017 and August 28, 2017 through September 5, 2017.

	• The previous notifications were based on findings from security firms and a report from a Payment Card Forensic Investigator ("PFI") engaged by the Organization. • In mid-October 2017, the investigation found that payment card information used on the e-commerce website may have been compromised during a longer period of time than initially determined and reported; specifically, during the period from October 26, 2016 through October 13, 2017 and October 15-19, 2017. • The Organization reported the incident(s) were discovered as a result of "working with computer security firms."
Affected individuals	The Organization estimates that 39,528 customers may have been affected by the incident, including 207 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Reported the incident to law enforcement. • Established a dedicated call center to answer any questions that individuals may have regarding the incident. • Continues to work with three security firms and has implemented enhanced security measures, including installing a new website security platform, implementing a security information and event management system (SIEM), and implementing enhanced logging.
Steps taken to notify individuals of the incident	Potentially affected individuals were notified in writing on November 27, 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.	The Organization reported "Customer credit and debit card accounts could be used fraudulently by the unauthorized individuals who obtain the payment card information. Most payment card issuers, however, will reimburse cardholders for any fraudulent charges on the accounts. Further, [the Organization] offerred in its notification letters to reimburse customers for any reasonble [sic], documents charges that their card issuers decline to reimburse." In my view, the financial information at issue (including payment card numbers, security codes and expiry dates) could be used to cause the harms of financial loss, fraud and identity theft. Email addresses could be used for phishing purposes. 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 "There is a reasonable likelihood that the perpetrators of the malware incident will attempt tio [sic] use the stolen card data to make fraudulent charges or will sell the data to other criminals who will attempt such fraud. As noted above however, the harm should be only temporary and any fraud on the customers' accounts should be reimbursed by the card issuers or may be reimbursed by [the Organization]." 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 almost one year. 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 harms of financial loss, fraud and identity theft. Email addresses could be used for phishing purposes. These are significant harms. 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 almost one year.

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 in writing on November 27, 2017 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner