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	Silver Bridge Funding, Inc., operating as Universal Business Team (Organization)
Decision number (file number)	P2017-ND-75 (File #005612)
Date notice received by OIPC	May 15, 2017
Date Organization last provided information	May 30, 2017
Date of decision	June 9, 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 an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • billing address, • shipping address, • email address, • credit card number, expiry date, CVV number, and • website password. 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 e-commerce website.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• On or around August 24, 2016, hackers inserted malware into the software supporting the Organization's website www.ubteam.com

	• The malware was present until on or around January 9, 2017 when it was discovered by a third party cyber security specialist.
Affected individuals	The Organization reported the incident may have affected approximately 500 individuals in Canada, including 37 in Alberta.
Steps taken to reduce risk of harm to individuals	• Quarantined the malware. • Disabled credit card processing on the website. • Identified the rogue software, completed an audit report, and implemented security enhancements. • Reported incident to privacy commissioners of British Columbia, Canada and Quebec.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter sent between May 15, 2017 and May 19, 2017.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 "Fraud, financial loss, negative effects on a credit record, identity theft, loss of password and phishing may result from the breach." I agree with the Organization. The financial information at issue could be used to cause the harms of identity theft, fraud, financial loss and negative effect on a credit record. Email addresses and credentials (website password) could be used for phishing purposes, or to compromise other online accounts with the same password. 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 "The likelihood that harm could result from this breach is high because the incident resulted from malicious intent. The information, which is sensitive, was potentially exposed for approximately three to four months." I agree with the Organization's assessment. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and malware). The information was potentially exposed for three to four months.
DECISION UNDER SECTION 37.1(1) OF PIPA	
Based on the information provided by the Organization and given the circumstances, I have decided that there is a real risk of significant harm to the affected individuals as a result of this incident. The financial information at issue could be used to cause the harms of identity theft, fraud, financial loss and negative effect on a credit record. Email addresses and credentials (website password) could be used for phishing purposes, or to compromise other online accounts with the same password. These are all significant harms. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and malware). The information was potentially exposed for three to four months.	

I require the Organization to notify affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation.*

I understand the Organization notified affected individuals by letter sent between May 15, 2017 and May 19, 2017. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner