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	PLAE Inc. (Organization)
Decision number (file number)	P2018-ND-063 (File #008947)
Date notice received by OIPC	June 14, 2018
Date Organization last provided information	June 14, 2018
Date of decision	June 19, 2018
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) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, • telephone number, • email address, • credit card number and related 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 in Alberta via the Organization's e-commerce website, PLAE.CO.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On May 10, 2018, the Organization discovered a cyber-attack on its PLAE.CO website that may have affected customers who placed online orders between March 15, 2018 and May 11, 2018. • The incident "was identified by orders failing for credit cards."
Affected individuals	The incident affected 3 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Launched a detailed forensic investigation and took steps to close the security vulnerability. • Partnering with the United States Secret Service and various financial institutions to further the investigation. • Terminated the cyberattack and took steps to improve efforts to keep PLAE.CO secure and free from threats and vulnerabilities.
Steps taken to notify individuals of the incident	The Organization reported a notification letter was sent June 4, 2018 via email and on June 6, 2018 via US mail.
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 the type of harm that might result from this breach as "Potential financial loss". In my view, the financial information at issue could be used to cause the significant harms of fraud, identity theft and financial loss. Email address could be used for phishing. I have previously found phishing to be a significant harm.
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 of harm resulting from this incident as "Moderate - we are uncertain of successful transmission of data to the unauthorized person". 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 (cyberattack). Further, the information may have been exposed for approximately two months.
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 could be used to cause the significant harms of fraud, identity theft and financial loss. Email address could be used for phishing. I have previously found phishing to be a significant harm. 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 (cyberattack). Further, the information may have been exposed for approximately two months.

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 letter sent June 4, 2018 via email and on June 6, 2018 via US mail. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner