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	Eye Safety Systems, Inc. (Organization)
Decision number (file number)	P2020-ND-007 (File #013753)
Date notice received by OIPC	October 29, 2019
Date Organization last provided information	October 29, 2019
Date of decision	February 11, 2020
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the individuals 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 a U.S. based online retailer and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The information at issue includes: • name, • billing address, • credit/debit card number, CVV code, and expiration date. 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 website esseyepro.com. The Organization maintains "…that it is not subject to the jurisdiction of the Office of the Information & Privacy Commissioner of Alberta". In my view, given the Organization is an "organization" as defined in PIPA, and the information at issue qualifies as "personal information" as defined in PIPA, PIPA applies to the extent the information was collected in Alberta.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On July 16, 2019, a third-party developer reported unusual activity in email logs and determined that emails had been sent from the server hosting the Organization's website, to an unauthorized email address. • The Organization investigated and concluded that an unauthorized individual or group extracted personal information by executing a vulnerability in the website code. • The unauthorized person was able to obtain the information starting on or around November 21, 2017, and ending on July 16, 2019.
Affected individuals	The incident affected 16 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Investigated and began efforts stop further unauthorized access to information. • Removed the website from use, preventing any further access and took additional steps to block further unauthorized access. • Planning to re-engineer the process in which payment information is collected on the website. • Continuing to review, audit, and improve security controls and processes. • Provided affected individuals with 24 months of free identity protection services.
Steps taken to notify individuals of the incident	The Organization reported that it would be notifying affected individuals by letter sent October 28, 2019
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 specifically identify potential harms that might result from this breach, but its notice to affected individuals said "We encourage you to remain vigilant for incidents of fraud and identity theft…". In my view, a reasonable person would consider that the contact and financial information 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 did not assess the likelihood of harm resulting from this incident. In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach appears to be the result of malicious intent (deliberate action) and the personal information at issue was extracted. Personal information was exposed for over a year and a half.

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.

A reasonable person would consider that the contact and financial information 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 appears to be the result of malicious intent (deliberate action) and the personal information at issue was extracted. Personal information was exposed for over a year and a half.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand individuals were notified by letter sent October 28, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner