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 Buy Direct, Inc. (Organization)
Decision number (file number)	P2020-ND-118 (File #013630)
Date notice received by OIPC	October 11, 2019
Date Organization last provided information	October 11, 2019
Date of decision	October 27, 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 those 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 an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident may have involved the following information: • name, • mailing address, • email address, • prescription information, • payment card number, verification code, and expiry date. 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 ecommerce website, www.eyebuydirect.com.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• In June 2019, the Organization learned that a number of US consumers had reported fraudulent activity on their credit cards. The consumers had all made transactions on the Organization's website. • The Organization investigated and concluded its systems showed signs of intrusions; however, investigators were unable to confirm with certainty how or when the platform had been breached or whether any data had been accessed or taken. • The Organization notified individuals who made purchases on the website between September, 2018 and September 2019.
Affected individuals	The incident may have affected approximately 80,000 Canadians.
Steps taken to reduce risk of harm to individuals	• Investigated and retained an independent cyber security firm to help review and update security protections across all systems. • Addressed the incident and corrected identified weaknesses, including further consolidating the security of the platform. • Reported the incident to relevant data protection authorities.
Steps taken to notify individuals of the incident	Affected individuals in Canada were notified by email on October 12, 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 harm(s) that might result from the breach, but its notification to affected individuals advised them to "…check the statements of any credit card you used to make a purchase on the [Organization's] website for fraudulent or suspicious charges. If you find even one, contact your credit card company immediately and report the fraud." In my view, a reasonable person would consider the contact, transaction and financial information at issue could be used to cause the significant harms of identity theft and fraud. Email address could be used for phishing purposes, increasing vulnerability to 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	The Organization reported "Given the fact that the forensic investigators were unable to confirm with certainty how or when the platform had been breached or whether any customer data had been accessed or taken, [the Organization], in an abundance of caution, has made the decision to notify all customers who made purchases…".

between the incident and the possible harm.	In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unauthorized third party (deliberate intrusion) and it appears the compromised information may have been used for fraudulent purposes in some cases. The Organization cannot confirm information was not exfiltrated. Further, the information may have been exposed for up to a year.

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 the contact, transaction and financial information at issue could be used to cause the significant harms of identity theft and fraud. Email address could be used for phishing purposes, increasing vulnerability to identity theft and fraud. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unauthorized third party (deliberate intrusion) and it appears the compromised information may have been used for fraudulent purposes in some cases. The Organization cannot confirm information was not exfiltrated. Further, the information may have been exposed for up to a year.

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 the Organization notified affected individuals in Canada by email on October 12, 2019. The Organization is not required to notify affected individual again.

Jill Clayton
Information and Privacy Commissioner