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	EZYield (Organization)
Decision number (file number)	P2014-ND-08 (File #P2565)
Date notice received by OIPC	January 6, 2014
Date Organization last provided information	January 6, 2014
Date of decision	September 2, 2014
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify affected individuals pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	I have jurisdiction because the Organization is an "organization" as defined in section 1(1)(i)(i) and the information of Albertans was affected.
Section 1(1)(k) of PIPA "personal information"	The incident involved all of the following information about the affected individuals: • name • credit card information, including CVV code, credit card number and expiration date. This information is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ☒ unauthorized disclosure	

Description of incident	• An online application hosted and operated by the Organization was the subject of a cyber-attack. • The attack was discovered on October 24, 2013. • The name and credit card information of six (6) Albertans was compromised.
Affected individuals	• Six (6) individuals in Alberta were affected.
Steps taken to reduce risk of harm to individuals	• Upon discovery of the security incident, the Organization launched an internal investigation. • The access point used by the cyber attacker to gain access to information was shut down. • The Organization acquired the services of a data security specialist to assist in the investigation of the incident. • Independent third party computer forensics experts were hired to determine the scope of the incident. • The six (6) Albertans that were impacted were notified. • Each of the affected individuals was provided with one (1) year free credit monitoring and identity restoration services. • The Organization also provided affected individuals with information on protecting against identify theft and fraud. • Written notification of the incident was provided to national consumer regulation agencies and other United States state regulators as the Organization is US-based. • Major credit card brands were notified of the incident.
Steps taken to notify individuals of the incident	• Written notification was sent to each of the six (6) Albertans affected by the breach.
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 recognized that the affected individuals may be at risk of identity theft, fraud and/or financial loss. In my view, the personal information involved is highly sensitive. The types of harm that could result from unauthorized access to this information include identity theft, fraud and financial loss. In my view, these are significant harms.
Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture.	The Organization reported that due to the sensitivity of the information involved, there was a real risk of significant harm to the affected individuals. In my view, the likelihood of harm resulting from this incident

There must be a cause and effect relationship between the incident and the possible harm.	is increased because the personal information of the affected individuals was accessed by an unauthorized individual(s) through a deliberate cyber-attack.

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 determined that there is a real risk of significant harm to the affected individuals. My determination is based on the fact that the personal information involved is sensitive identity and financial information including name, credit card information (credit card number, CVV code and expiration date). The incident is the result of a deliberate cyber-attack.

I understand the Organization has notified the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). The Organization is, therefore, not required to notify these individuals again.

Jill Clayton
Information and Privacy Commissioner