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	EVO Payments International Corp. - Canada (Organization)
Decision number (file number)	P2017-ND-39 (File #002257)
Date notice received by OIPC	January 29, 2016
Date Organization last provided information	January 29, 2016
Date of decision	March 6, 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 a payment processing company headquartered in the USA, and 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, • social insurance number, • date of birth, • address, • primary telephone number, and • passport or other government issued identification number. This information is about current and former sales agents in Canada and Alberta, and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On December 8, 2015, the Organization was informed by another company that a former employee of the Organization had accessed an electronic file containing the information at issue. • The former employee had been employed with the Organization between July and October 2014 and was not authorized to access the file. • The Organization's investigation confirmed that the information of 41 former and current independent sales agents was used to commit fraud (opening fraudulent accounts for mobile phone services or to purchase smart phones).
Affected individuals	A total of 841 Canadians were affected by the incident, including 60 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Initiated an internal investigation. • Reported the incident to law enforcement. • Confirmed with the other company that all fraudulent accounts have been closed and all records pertaining to the Organization's sales agents were purged from systems and relevant credit bureau records. • Reviewed internal access protocols and data collection practices. • Reminded employees of importance of maintaining security and confidentiality. • Established a toll free dedicated hot line that the affected individuals can call if they have any questions or concerns.
Steps taken to notify individuals of the incident	Affected individuals were notified on or around January 29, 2016.
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 information of 41 … former and current independent sales agents' information was used to commit fraud (i.e. opening fraudulent accounts or purchasing smart phones)." In my view, the identity information at issue could be used to cause the harms of identity theft, fraud and financial loss. These are 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.	As noted above, the Organization reported the information "was used to commit fraud." In my view, the likelihood of harm is increased because the incident resulted from malicious intent (unauthorized access and theft of the information), the information was exposed for a considerable length of time, and was used for fraudulent purposes.

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 identity information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. The likelihood of harm is increased because the incident resulted from malicious intent (unauthorized access and theft of the information), the information was exposed for a considerable length of time, and was used for fraudulent purposes.

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

I understand that the Organization notified affected individuals directly, on or around January 29, 2016. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner