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	ABS-CBN Canada Remittance Inc. (Organization)
Decision number (file number)	P2016-ND-31 (Case File #000052)
Date notice received by OIPC	November 27, 2014
Date Organization last provided information	February 18, 2015
Date of decision	May 30, 2016
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 incorporated in Ontario, Canada 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 all or some of the following information: • name, • address, • email address, • telephone number, • occupation, • identification document and number, place of issue, date of issue and expiry date (if social insurance number was listed, only last four digits recorded), and • information about whether an individual or family member is a "politically exposed foreign person". 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.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization is a money remittance business in Canada. Individuals in various countries are able to send money to beneficiaries who are located in the Philippines. The Organization operates through a network of accredited agents in Canada. • Accredited agents use a web-based system known as the Global Operations Management System (GOMS) to process transactions. • On October 9, 2014, an authorized agent in Calgary noticed two transactions on its daily transaction list that were not processed by that agent. After reviewing additional transaction lists, the agent identified thirty-three (33) suspected fraudulent transactions. • On October 19, 2014, the Organization identified an additional four (4) suspicious transactions that had been entered using a second agent's credentials. • The Organization reported that "fraudsters were able to access the two agents' sign-on credentials" and as a result accessed the personal information of twenty individuals. This information was successfully used to process fraudulent transactions.
Affected individuals	Twenty residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Reported the incident to the Calgary Police Service on October 28, 2014. • The two agents who were compromised were instructed to change their access credentials. • All agents have now been issued RSA tokens, and the system now requires two factor authentication. • The Organization implemented new head office security procedures to check IP addresses in relation to transactions and manual checking of transactions to detect potential intrusion attempts. • Engaged a private investigator to assist in tracing fraudulent transactions. • Retained IT experts to make recommendations to improve security.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on November 24, 2014.

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 that the information at issue could be used for identity theft. I agree with the Organization. The personal information at issue includes sensitive identity information that could be used to cause harm in the form of identity theft and/or fraud. 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.	The Organization reported that as of February 14, 2015, it had not received any complaints of identity theft or financial fraud from any of the 20 affected individuals. In my view, there is a real risk of significant harm resulting from this incident. The incident resulted from a deliberate attempt to obtain unauthorized access to personal information. The information was successfully used to process fraudulent transactions.
DECISION UNDER SECTION 37.1(1) OF PIPA	
Based on the information provided by the Organization and given the circumstances of this incident, I have decided that there is a real risk of significant harm to the affected individuals. The personal information at issue includes sensitive identity information that could be used to cause the significant harms of identity theft and/or fraud. The incident resulted from a deliberate attempt to obtain unauthorized access to personal information. The information was successfully used to process fraudulent transactions. The Organization notified the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) on November 25, 2014. The Organization is, therefore not required to notify the affected individuals again.	

Jill Clayton
Information and Privacy Commissioner