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	Infosat Communications GP Inc. (Organization)
Decision number (file number)	P2015-ND-34 (Case File #P2746)
Date notice received by OIPC	June 11, 2014
Date Organization last provided information	June 11, 2014
Date of decision	May 19, 2015
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 Alberta. I have jurisdiction because the Organization 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, • address, • postal code, • telephone number, • Global Positioning System (GPS) coordinates, • credit card number of two individuals, • Social Insurance Number (SIN) of one individual. This information is "personal information" as defined in section 1(1)(k) of PIPA and was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• Between May 2014 and June 5, 2014, an unauthorized individual gained access to the Organization's database containing personal information. • The Organization was notified of the incident by one of its dealers whose customers' information was compromised. • The intruder used a developer's account on a business application (web portal) to access the database. • The intruder collected the credit card numbers and card verification codes of three individuals, as well as the Social Insurance Number of one individual. • Unauthorized purchases were made using the credit cards numbers.
Affected individuals	Twenty-seven (27) Albertans were affected.
Steps taken to reduce risk of harm to individuals	• The web portal that was used to gain access to the database was immediately shut down upon the discovery of the incident. It was later decommissioned. • Credit card information is automatically deleted from the Organization's database once payment processing is completed. • Card verification code is not collected. • A new web portal with improved security controls has been implemented.
Steps taken to notify individuals of the incident	All 27 affected individuals were notified via telephone calls.
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 the affected individuals may be at risk of identity theft and financial fraud. In my view, the personal information involved is sensitive. It includes identity and financial information. The types of harm that could result from unauthorized access to this information are identity theft and financial fraud. 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. There must be a cause and effect relationship between the	The Organization reported that there is a real risk of significant harm to the affected individuals. In my view, the likelihood of harm resulting from this incident is increased because the personal and financial information was accessed by unauthorized individuals with malicious intent. The Organization reported that unauthorized purchases were made

incident and the possible harm.	using the credit cards numbers of some individuals affected by the incident.

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 involves sensitive identity and financial information of the affected individuals. The information was accessed by unauthorized individuals with malicious intent. The Organization reported that unauthorized purchases were made using the personal information of some of the individuals affected by the incident. These factors contributed significantly to my decision.

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

I understand the Organization notified the individuals who were affected, in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner