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	Copart Inc. (Organization).
Decision number (file number)	P2016-ND-40 (File #000963)
Date notice received by OIPC	June 2, 2015
Date Organization last provided information	June 2, 2015
Date of decision	August 16, 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 an "organization" as defined in section 1(1)(i)(i) of PIPA whose Canadian office is in Calgary Alberta.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, • driver's license number, • telephone number, • email address, • passport number, • account username and password. 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	• On March 31, 2015, the Organization discovered that an unauthorized person had gained access to its computer network. • The Organization engaged a leading cybersecurity firm to help determine what occurred and assist it in implementing enhanced security measures.
Affected individuals	A total of 313 individuals affected are residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Offered one year of Equifax Identity protection services to potentially affected customers, at no cost to the customer, in order to safeguard against misuse of credit card information. • Notified credit card merchant providers, so that issuing banks could monitor accounts and investigate. • Cooperated with law enforcement to identify and prosecute the criminal attackers. • Is continuing to improve security controls, including planned deployment of chip and-pin and tokenization.
Steps taken to notify individuals of the incident	The Organization notified all affected individuals by letter sent on October 27, 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 recognized that the type of harm that may result from the breach is identity theft and fraud. I agree with the Organization's assessment. The personal information at issue includes sensitive identity and credential information, as well as email addresses. This information could be used to cause the harms of identity theft, fraud and phishing. 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 did not specifically assess the likelihood of harm resulting from this incident, but reported that "given the nature of the incident and the type of information involved" it was notifying all members whose information may have been accessed. In my view, the likelihood of harm resulting from this incident is increased as it was the result of malicious intent (deliberate intrusion), and considering the number of individuals potentially affected.

DECISION UNDER SECTION 37.1(1) OF PIPA

Based on the information provided by the Organization I have decided that there is a real risk of significant harm to the affected individuals. The personal information at issue includes sensitive identity and credential information, as well as email addresses, which could be used to cause the significant harms of identity theft, fraud and phishing. The likelihood of harm resulting from this incident is increased as it was the result of malicious intent (deliberate intrusion), and considering the number of individuals potentially affected.

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 affected individuals by letter in compliance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner