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	Bell Helicopter Textron Inc. (Organization)
Decision number (file number)	P2015-ND-12 (File #P2423)
Date notice received by OIPC	August 20, 2013
Date Organization last provided information	May 30, 2014
Date of decision	March 17, 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 the State of Delaware, USA. 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 all or some of the following information: • name, • email address, • credit card numbers. This information is "personal information" as defined in section 1(1)(k) of PIPA, and was collected from residents of Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization learned that a phishing email containing a malicious link was sent to some training program attendees. The email appeared to originate from the Organization. • The Organization determined that an unauthorized third party exploited a vulnerability and was able to access training attendees' names and email addresses, stored in a database. • The same database also contained credit card numbers. The Organization was not able to determine whether these were for personal or corporate cards, although it believes most were for corporate cards. The Organization was able to determine that the credit card numbers had expired. • The Organization's database audit logs contained no evidence that credit card information was accessed.
Affected individuals	Five residents of Alberta.
Steps taken to reduce risk of harm to individuals	The Organization conducted an investigation and warned the attendees about the fraudulent phishing email.
Steps taken to notify individuals of the incident	Affected individuals were notified on July 12 and 13, 2013.
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 attendees' names and email addresses could be used to send a phishing email, luring recipients to a fraudulent website. The Organization did not identify the possible harms that could result from access to expired credit card numbers. In my view, names and credit card numbers could be used to cause harm in the form of identity theft and/or fraud. Expired credit card numbers could be used in conjunction with email addresses for phishing purposes. 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 the credit card numbers had expired, and further, that audit logs "contained no evidence that credit card information was accessed." The Organization also reported that some training attendees received a phishing email. In my view, there is a real risk of significant harm resulting from this incident. Some training attendees did receive a phishing email. Even though the credit card numbers had expired, this information, used in a phishing scam, could make affected individuals more vulnerable to fraud. Further, the incident was caused by malicious intent.

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 could be used to cause the significant harms of identity theft/fraud and phishing. The incident was the result of malicious intent and some of the affected individuals did receive phishing emails containing a malicious link. The Organization notified the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) on July 12 and 13, 2013. The Organization is, therefore not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner