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	Calder Bateman Communications Ltd. (Organization)
Decision number (file number)	P2019-ND-142 (File #005091)
Date notice received by OIPC	February 28, 2017
Date Organization last provided information	May 19, 2017
Date of decision	August 16, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA), the Organization is required to notify the individuals whose personal information was collected in Alberta.
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is incorporated and operating in Alberta, 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, • credit card type, • credit card number, • cardholder name, • credit card expiry date, and • card verification value (CVV). 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 runs all aspects of the Full House Lottery on behalf of hospital foundations.

	• On February 22, 2017, the Organization's service provider, Pixel Army, discovered that an unauthorized party remotely accessed its website on February 9, 2017 and installed malware aimed at capturing the personal information of individuals using the Organization's website. • The Organization contracted a cybersecurity firm to investigate the incident in cooperation with the service provider that was maintaining the website. • The Organization and its service provider took steps to remove the malware and to enhance website security to prevent reoccurrence.
Affected individuals	The incident affected 3,350 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Reported the incident to the Office of the Information and Privacy Commissioner of Alberta. • Reported the incident to credit card issuers. • Reported the issue to law enforcement as well as Alberta Gaming and Liquor Commission.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on February 24, 2017. Some individuals were notified by telephone.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury – that could be caused to those 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.	In assessing the potential harm(s) that might result from this incident, the Organization reported: *The primary risks are:* • *fraudulent activity on individuals' credit cards* • *potential for financial loss* • *potential impact on credit records* • *identity theft* In my view, a reasonable person would consider that the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud.
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: *We believe there was malicious intent - for example, the hacker may intend to re-sell the information to others who in turn may try to use the information for criminal purpuses [sic].*

	The information is sensitive from a credit perspective, which is very serious. However, it was not sensitive in terms of health or other such personal information. *As referenced, a factor which may help obviate this risk is the duration of the breach - however, it still means that the perpetrator could have had access to the information of some purchasers for 13 days before the breach was discovered.* *To this time, we have directly been advised by three or four individuals of potential false charges to a credit card - these have not been verified.* In my view, a reasonable person would consider that the likelihood of harm resulting from this breach is increased because it resulted from malicious intent (deliberate intrusion and malware). The information was exposed for 13 days before the breach was discovered.

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.

A reasonable person would consider that the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this breach is increased because it resulted from malicious intent (deliberate intrusion and malware). The information was exposed for 13 days before the breach was discovered.

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

I understand the Organization notified the affected individuals by email on February 24, 2017, in accordance with the Regulation. The Organization is, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner