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-143 (File #005561)
Date notice received by OIPC	May 9, 2017
Date Organization last provided information	May 24, 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 affected individuals.
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, • email address, • telephone number, • gender, • age, and • amount of purchase, • 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 via the Organization's website and at show homes.

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 May 2, 2017, the Organization's service provider discovered that system performance was affected by malware. • This new incident related to an earlier incident, for which certain vulnerabilities remained undetected and therefore unaddressed. • The vulnerability affected transactions conducted through the Organization's website between February 23 and May 2, 2017. • The Organization suspended all transactions, and worked with a cybersecurity company to address the issues left from the previous incident. • The Organization and its service provider then took steps to enhance information security and prevent reoccurrence.
Affected individuals	The incident affected 29,014 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 law enforcement and payment processors. • Reported the incident to credit card issuers.
Steps taken to notify individuals of the incident	Affected individuals were notified by email and letter on May 5, 2017. The Organization also issued a news release to inform the public.
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.	In assessing the potential harm(s) that might result from this incident, the Organization reported: *The primary risks are:* • *fraudulent activity on personal 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. Email addresses could be used for phishing purposes, increasing vulnerability to 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 purposes.* *The information is sensitive from a credit perspective, which is serious. However, it was not sensitive from health or other such personal perspectives.* *The perpetrator had access to the information for over two months.* *…No individuals under 18 are allowed to purchase lottery tickets. There will have been some seniors but those will very likely have been "independent" individuals able to make their own financial decisions.* 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 over 2 months.

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. Email addresses could be used for phishing purposes, increasing vulnerability to 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 over 2 months.

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 affected individuals by email and letter on May 5, 2017 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton