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	Eddie Bauer LLC (Organization)
Decision number (file number)	P2016-ND-47 (File #003545)
Date notice received by OIPC	August 19, 2016
Date Organization last provided information	August 19, 2016
Date of decision	August 23, 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"	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, • payment card number, security code, expiry date. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was accessed through the Organization's point of sale systems used in its retail stores, including stores in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On July 15, 2016, a forensics firm retained by the Organization identified evidence that malware was present on many of the Organization's point of sale registers.

	• The Organization believes the malware was installed by an unknown third party between January 2, 2016 and July 17, 2016, enabling unauthorized parties to access names and payment card data. Payment information used on the Organization's ecommerce website was not affected. • On July 18, 2016, the Organization alerted all employees with email access to the possibility of social engineering attacks, and asking personnel to contact security to report any such activity. • The Organization's IT team blocked certain IP addresses and URLs across the enterprise; required password changes for all domain admin accounts and certain service accounts; implemented blocking on Word macros and Adobe Flash; and began increased enterprise monitoring. • On the following day, after effective containment actions were taken, social engineering attempts were thwarted by employees and security. • On July 19, 2016, an email was received by a store manager in Ontario complaining about service in the store, and asking the manager to open an attached word document to review "details" of a complaint. The email was subsequently found to be identical to a phishing message in another FBI case, which indicated that the attacker had been locked out of the system and was attempting to regain access.
Affected individuals	A total of 136, 366 Canadians may have been affected, including 32,180 in Alberta.
Steps taken to reduce risk of harm to individuals	• Immediately initiated incident and containment protocol and launched an investigation that included the commissioning of third-party forensic experts and contacting the U.S. Federal Bureau of Investigation. • Notified payment card networks to coordinate with card issuing banks to monitor for fraudulent activity on cards used during the relevant time period . • Enhanced security of point of sale systems.
Steps taken to notify individuals of the incident	The Organization in the process of alerting all 225,000 customers whose information may have been affected. The Organization provided a copy of its written notification with its breach report.

REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 its report of the incident, the Organization did not specifically identify any possible harm that might result, but its draft notice to affected parties did offer "identity protection services" and made reference to "monitor[ing] for fraudulent activity on cards". In my view, the information involved in this incident could be used to cause the harms of identity theft, fraud and financial loss. 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 noted in its report that "Given that [the Organization's] point of sale systems were affected by malware, and the involvement of payment information, [the Organization] is of the view that the test for mandatory breach reporting under the *Personal Information Protection Act* (Alberta) is met". In my view, there is a real risk that significant harm might result from this incident. The likelihood of harm is increased because the incident was the result of a deliberate intrusion by an unauthorized party. The social engineering attempts subsequent to containment actions indicate a persistent, deliberate attacker. Further, the malware was installed sometime between January 2, 2016 and July 17, 2016 which means the information may have been exposed for a considerable length of time.

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.

The information involved in this incident could be used to cause the significant harms of identity theft, fraud and financial loss. The likelihood of harm is increased because the incident was the result of a deliberate intrusion by an unauthorized party. The social engineering attempts subsequent to containment actions indicate a persistent, deliberate attack. Further, the malware was installed sometime between January 2, 2016 and July 17, 2016 which means the information may have been exposed for a considerable length of time.

I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) and provide me with written confirmation that it has done so on or before September 9, 2016.

I understand the Organization in the process of alerting all 225,000 customers whose information may have been affected.

Jill Clayton
Information and Privacy Commissioner