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	Bailey's, Inc. (the Organization)
Decision number (file number)	P2016-ND-38 (File #002718)
Date notice received by OIPC	March 17, 2016
Date Organization last provided information	March 17, 2016
Date of decision	July 25, 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 a United States based company 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 the following information: • name, • address, • telephone number, • email address, • log-in and password, • credit card number, expiration date, CCV, and • additional information related to online orders. 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	• In January 2016, the Organization learned its online e-commerce website had been hacked and a keystroke recorder installed. • After an extensive investigation, the Organization learned the cyber-attack had first occurred in December 2011.
Affected individuals	Approximately 250,000 individuals in total are affected, including 7,000 in Canada and 641 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Immediately initiated a forensic investigation. • Engaged a security consultant and continue to implement recommendations to strengthen firewall and address vulnerabilities, including revoking, changing and renewing passwords, replacing server. • Notified police, FTC, banks and credit card companies.
Steps taken to notify individuals of the incident	Affected individuals were notified by email and mail, between March 7, 2016 and April 4, 2016.
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 the potential harm that could result from this incident included "Fraudulent use of credit cards. Login's [sic] and Passwords were also taken. The risk there is that some people use the same Log/Pass for their Bank, and then use it everywhere else they go. So there is some exposure but the extent of it is unknown." I agree with the Organization. The credit card information could be used to cause the harms of identity theft, fraud, and financial loss. Email addresses could be used for phishing purposes. Log-ins and passwords could be used to compromise other accounts. 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 risk to the [credit card information] is high because we are seeing them used fraudulently as are the Banks." The Organization also noted there was evidence of malicious intent and "Encryption was/is, in place. But keystroke readers watch people as they type." I agree with the Organization's assessment. The likelihood of harm resulting from this incident is increased because it was caused by deliberate action, indicating malicious intent. Further, the information was 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 credit card information could be used to cause the harms of identity theft, fraud, and financial loss. Email addresses could be used for phishing purposes. Log-ins and passwords could be used to compromise other accounts. These are significant harms. The likelihood of harm resulting from this incident is increased because it was caused by deliberate action, indicating malicious intent. Further, the information was exposed for a considerable length of time. 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 between March 7, 2016 and April 4, 2016 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner