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	Crocs Canada Inc. (Organization)
Decision number (file number)	P2016-ND-28 (Case File #000864)
Date notice received by OIPC	May 22, 2015
Date Organization last provided information	March 21, 2016
Date of decision	May 3, 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 registered in Alberta as an Extra-Provincial Corporation and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The following information was involved in this incident: • first and last name, • username and password, • shipping address, • billing address, • telephone number, and • email address. 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	• On April 15, 2015, after a forensic investigation, the Organization learned that individuals may have obtained unauthorized access to information stored on a number of servers. • The Organization had initiated the investigation after learning of potential vulnerabilities pursuant to a penetration test. • The investigation confirmed that between November 2014 and March 2015, individuals obtained unauthorized access to the Organization's servers to obtain certain information from the website. • The vulnerability allowed SQL injections to retrieve certain user data.
Affected individuals	A total of 24 Canadians were affected, 3 of whom reside in Alberta.
Steps taken to reduce risk of harm to individuals	• The Organization engaged a computer forensic expert to investigate and address the incident. • All affected individuals were notified of the incident and advised of the steps to take in order to reduce the chance of any adverse effects from the incident. • Affected servers were taken offline to eliminate the vulnerability. • The Organization stated additional security measures will be implemented as appropriate.
Steps taken to notify individuals of the incident	Notification was sent by email on or around May 21, 2015.
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 noted that the information at issue "is not highly sensitive"; however, the Organization recognized that "if users use the same username and password combination on multiple websites, it is possible that other Internet accounts could be accessed as a result of the incident." I agree with the Organization's assessment. The information at issue could be used to gain unauthorized access to other internet accounts. In addition, email addresses could be used to cause the significant harm of phishing.

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 assessed the risk of harm resulting from this incident to be low "because there is no evidence that any sensitive personal information or financial account information was involved in the incident." In my view, there is a real risk that harm will result from this incident. The incident was the result of malicious intent. Further, the Organization acknowledged in its letter notifying affected individuals that although the investigation provided evidence of access between November 2014 and March 2015, access could have occurred earlier. The longer information is exposed to unauthorized parties, the greater this risk.

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 personal information at issue could be used to gain unauthorized access to other internet accounts and could be used to cause the significant harm of phishing. The incident was the result of malicious intent. Further, the Organization acknowledged in its letter notifying affected individuals that although the investigation provided evidence of access between November 2014 and March 2015, access could have occurred earlier. The longer information is exposed to unauthorized parties, the greater this risk.

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).

I understand the Organization notified the affected individuals on May 21, 2015. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner