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	Ikea Canada Ltd. (Organization)
Decision number (file number)	P2016-ND-43 (File #000967)
Date notice received by OIPC	June 8, 2015
Date Organization last provided information	March 08, 2016
Date of decision	August 17, 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 incorporated 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"	Some or all of the following information was involved in this incident: • name, • home address (if provided), • telephone number (if provided), and • cell phone number (if provided). 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 May 25, 2015 an unauthorized third party was able to access certain data elements on the Organization's website via a previously unknown vulnerability. • The Organization's ongoing monitoring activities enabled the prompt identification and detection of the unauthorized activity on the same day (May 25). • The Organization immediately commenced an investigation. • The vulnerability was temporarily remediated within 2 hours of detection and within 5 hours of detection a permanent code fix was in place.
Affected individuals	A total of 622 Canadians were affected by this incident, including 34 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Provincial privacy regulatory authorities were informed in Quebec, British Columbia and Alberta. Foreign privacy regulatory authorities were also informed of the incident. • The incident was reported to law enforcement authorities. • A third party forensics firm was engaged to conduct a forensic analysis of the incident to determine what was accessed or accessible. • The Organization's privacy team in Canada was notified and was involved in the response strategy. • The Organization notified affected individuals globally.
Steps taken to notify individuals of the incident	Notification took place via email on June 5, 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.	The Organization reported there was no real risk of significant harm as the information is essentially "phone book information". In my view, the information at issue is of low sensitivity in that it does not include identity, financial, or medical information, and could, in some cases, be publicly available. Nonetheless, the information, particularly in combination, could be used to cause the harm of phishing, which can lead to other harms such as fraud. 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 it "has not received any customer complaints, and there has been no evidence of misuse of the personal information in question." In my view, there is a real risk the information at issue could be used to cause significant harm. Although the Organization was able to detect and permanently remediate the vulnerability very quickly, and there is no evidence of misuse of the information, the incident nonetheless was the result of malicious intent (deliberate intrusion). The circumstances in this case suggest the perpetrator could have intentionally targeted customer information with targeted phishing (i.e. spear phishing) in mind.

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 resulting from this incident. Although the information at issue is of low sensitivity, and could, in some cases, be publicly available, it could be used to cause the harm of phishing, which can lead to other harms such as fraud. These are significant harms. Although the Organization was able to detect and permanently remediate the vulnerability very quickly, and there is no evidence of misuse of the information, the incident nonetheless was the result of malicious intent (deliberate intrusion). The circumstances in this case suggest the perpetrator could have intentionally targeted customer information with targeted phishing (i.e. spear phishing) in mind.

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 by email on June 5, 2015. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner