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 Limited Partnership (Organization)
Decision number (file number)	P2018-ND-089 (File #007873)
Date notice received by OIPC	February 22, 2018
Date Organization last provided information	February 22, 2018
Date of decision	July 27, 2018
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the individual in Alberta pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization operates in Alberta and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • address, • telephone number, • delivery date, time of delivery, time of mattress pick-up, additional notes relating to the delivery, and • transaction information relating to a refund. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss	☒ unauthorized access ❑ unauthorized disclosure
Description of incident	• Between February 12, 2018 and February 15, 2018, the Organization received calls from thirteen (13) customers reporting that an alleged employee of the Organization had telephoned them with information relating to delivery, mattress pick-up, or a refund.

	• The Organization has no record of the named employee and no calls were authorized or condoned by the Organization. • In twelve (12) of the cases reported, the individual stated that in order to reschedule a delivery or mattress pick up, a charge would apply, and asked the customers for credit card information. The remaining one (1) customer was called in relation to a refund owing to the customer, and was also asked to provide credit card information. • In total, the individual was successful in obtaining credit card information from three (3) customers, including one resident of Alberta. • The Organization has audited access activity on the potential systems that were used to obtain the customers' information and no suspicious activity has been identified as of yet. The Organization has reached out to its third party delivery supplier who accesses customer data to investigate the source of the data breach. The cause of the breach is undetermined at the time of the Organization's report of the breach.
Affected individuals	The incident affected 13 individuals, including one (1) resident of Alberta.
Steps taken to reduce risk of harm to individuals	• Launched an internal investigation to determine the source of the breach through monitoring audit trails to identify suspicious activity and changing passwords. • Notified third party delivery supplier to obtain their assistance in investigating the source of the data breach. The third party supplier has engaged an investigator and also reset all passwords as a measure to help contain the breach and protect personal information. • Asked customers who divulged credit card information to the individual to immediately contact their financial institutions to report the incident and cancel their credit cards.
Steps taken to notify individuals of the incident	The Organization reported that "As the discovery of the breach was triggered by customers calling in to [the Organization's] customer service centre to report the incident, these customers were notified verbally that we are investigating this matter." Further, the Organization "intends to send a follow-up letter in writing to each of these cutomers [sic] to notify them that we are investigating this matter and taking steps to protect their information."

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 that "For the three customers whose credit card information was obtained by the individual, the risk of harm is financial loss and negative effects on their credit records. For the other customers, the risk of harm is potential identity theft if the information accessed can be used for phishing." Further, "In the three cases where customers divulged credit card information to the individual, the level of potential harm is high as this information could be used for fraudulent purchases and identity theft. In all other cases, the harm is low as the personal information obtained is of less sensitivity." Based on the Organization's report of this incident, it appears that an unknown individual had unauthorized access to customer contact and profile (purchase history) information, and, in at least three cases, used that information to obtain additional financial information (payment card information). Clearly the information at issue can and was used to cause the significant harms of fraud and spear 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 reported that "In the three cases where customers divulged credit card information to the individual, the likelihood that harm could result is low. While the information obtained was sensitive and likely obtained for the purpose of making fraudulent purchases using these customers' credit card information, the likelihood is low since these customers reported the incident shortly after they [sic] occurred and they were advised by [the Organization] to immediately contact their financial institutions to report the incident and cancel their credit cards. In other words, assuming that the customers contacted their financial institutions immediately after reporting the incident to [the Organization], the time from which the credit card information was obtained from the customers to the time customers reported the incident to their financial institutions and cancelled their credit cards was a short period of time. In all other cases, the likelihood that harm could result is low due to the low sensitivity of the information." The Organization also reported that "As of February 15, 2018, [the Organization] has not received any more calls from customers to indicate that the issue continues. Also, since the incident was discovered, [the Organization] has taken steps to ensure that the information is secure, including changing passwords, monitoring audit trails, and notifying its third party delivery supplier to ensure that they also take measures to safeguard the information including changing passwords and assigning an investigator."

	In my view, a reasonable person would consider that there exists a real risk of significant harm resulting from this breach. The breach is the result of malicious intent (deliberate, unauthorized access to information, impersonation and successful use of the information for spear phishing purposes in order to obtain credit card information). Although the Organization reported that the risk is low because the customers reported the incidents shortly after they occurred and they were advised to immediately contact their financial institutions to report the incident and cancel their credit cards, the Organization does not know the cause of the breach, whether the 13 customers who reported the incident are the only ones whose personal information was compromised, or even if these 13 customers all followed up with their financial institutions. The fact that the Organization has not received further reports of spear phishing or fraudulent use of the information does not mean there has not been any occurrences, nor does it mean that the personal information of other customers was not compromised.

DECISION UNDER SECTION 37.1(1) OF PIPA

Given the information reported by the Organization I have concluded that there is a real risk of significant harm in this case.

It appears that an unknown individual had unauthorized access to customer contact and profile (purchase history) information, and, in at least three cases, used that information to obtain additional financial information (payment card information). Clearly the information at issue can and was used to cause the significant harms of fraud and spear phishing.

The breach is the result of malicious intent (deliberate, unauthorized access to information, impersonation and successful use of the information for spear phishing purposes in order to obtain credit card information). Although the Organization reported that the risk is low because the customers reported the incidents shortly after they occurred and they were advised to immediately contact their financial institutions to report the incident and cancel their credit cards, the Organization does not know the cause of the breach, whether the 13 customers who reported the incident are the only ones whose personal information was compromised, or even if these 13 customers all followed up with their financial institutions. The fact that the Organization has not received further reports of spear phishing or fraudulent use of the information does not mean there has not been any occurrences, nor does it mean that the personal information of other customers was not compromised.

I require the Organization to notify the affected individual in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) **and confirm to my office within 10 days of the date of this decision that it has done so.**

Further, section 37.1(2) of PIPA states that "If the Commissioner requires an organization to notify individuals under subsection (1), the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate in addition to the requirements under subsection (1)."

Pursuant to section 37.1(2), I require the Organization to consider whether or not there may be additional affected individuals, beyond those who may have been identified to date. That is, the Organization has reported that it is aware of 13 individuals who have been targeted as a result of what appears to be unauthorized access to customer information. I am concerned that the personal information of additional customers may have been compromised. I understand that the Organization has audited access activity on the potential systems that were used to obtain the customers' information and no suspicious activity has been identified as of yet. Further, the cause of the breach was undetermined at the time of the Organization's report of the breach. I require the Organization to consider this scenario and advise me as to its assessment of the potential risk to other individuals, beyond those 13 who already reported incidents.

The Organization is required to provide me with its assessment of this possible additional risk, in writing, within 10 days of the date of this decision.

Jill Clayton
Information and Privacy Commissioner