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	Kohl's Department Stores Inc. (Organization)
Decision number (file number)	P2016-ND-46 (File #001805)
Date notice received by OIPC	September 30, 2015
Date Organization last provided information	July 8, 2016
Date of decision	August 22, 2016
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual 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 Organization reported the following information about one affected Albertan was involved in this incident: • name, • debit card number, • expiration date, and • CVV code. The Organization also reported that "No credit card information of the relevant Albertan was impacted." This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization reported that an Alberta billing address was used to place an order via its online system and it is likely the information at issue was transmitted from Alberta.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On August 17, 2015 the Organization discovered a call centre employee in Dallas, Texas was capturing names and debit card information for certain customers for unauthorized purposes. • The employee had been capturing customer information between February 17, 2015 and July 24, 2015. • The incident was discovered after two customers complained about potentially fraudulent charges on their debit cards which had been used to make payments against their Organization charge account balances.
Affected individuals	A total of 128 individuals across Canada and the USA were affected; of these, one individual was a resident of Alberta.
Steps taken to reduce risk of harm to individuals	• The Organization launched an investigation. • Terminated the call centre employee. • Reported the incident to law enforcement. • Arranged to provide free identity protection services to the affected individual for one year.
Steps taken to notify individuals of the incident	The Organization notified the affected Albertan in writing on September 29, 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 the sensitivity of the information at issue is "low to moderate" and that "potential harm to the affected customers includes fraudulent charges on the relevant debit cards." I agree with the Organization. The personal information involved includes financial information which 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 reported "there is a reasonable possibility that certain of the affected individuals may incur fraudulent charges on their debit cards"; however "The level of potential harm is low to moderate because certain laws, industry rules and standard industry practices limit a customer's liability for fraudulent charges." In my view, there is a real risk that significant harm might result to the affected individuals as a result of this incident. The likelihood of harm is increased because the personal

	information was deliberately accessed by an unauthorized party(s), and was exposed for approximately 5 months before the Organization became aware of the breach and notified affected individuals and law enforcement. The breach was only discovered after two customers complained about potentially fraudulent charges on their debit cards which had been used to make payments against their Organization charge account balances. The Organization can only speculate that affected individuals will have limited liability for fraudulent charges that may be incurred.

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 individual.

The personal information involved includes financial information which could be used to cause the significant harms of identity theft, fraud and financial loss. The likelihood of harm is increased because the personal information was deliberately accessed by an unauthorized party(s), and was exposed for approximately 5 months before the Organization became aware of the breach and notified affected individuals and law enforcement.

The breach was only discovered after two customers complained about potentially fraudulent charges on their debit cards which had been used to make payments against their Organization charge account balances. The Organization can only speculate that affected individuals will have limited liability for fraudulent charges that may be incurred.

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). I understand the Organization notified the affected Albertan in writing on September 29, 2015. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner