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	Hudson's Bay Company (Organization)
Decision number (file number)	P2018-ND-163 (File #008500)
Date notice received by OIPC	April 27, 2018
Date Organization last provided information	August 8, 2018
Date of decision	December 3, 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 those individuals whose information was collected in Alberta, pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • payment card number, and • expiration date. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected from individuals through certain point of sale systems at potentially all Saks Fifth Avenue, Saks OFF 5TH, and Lord & Taylor locations in North America. The Organization reported there are approximately three (3) stores in Alberta that may be impacted by this issue.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• Around July 1, 2017, malware began running on certain point of sale systems at potentially all Saks Fifth Avenue, Saks OFF 5TH, and Lord & Taylor locations in North America. The malware was designed to collect customer payment card information. • The breach was discovered on March 29, 2018. • The Organization contained the issue on March 31, 2018, and believes it no longer poses a risk to customers shopping at its stores.
Affected individuals	The Organization said it is not able to determine the number of Alberta residents who may have been affected by this incident and noted that "not all customers who shopped at the potentially impacted stores during the relevant time period were affected by this incident".
Steps taken to reduce risk of harm to individuals	• Engaged data security experts to conduct an investigation. • Working with law enforcement authorities and coordinating with the payment card companies. • Arranged with a credit reporting agency to provide potentially impacted customers with identity protection services at no cost. • Encouraged individuals to refer to their payment card statements to identify the payment card they may have used at affected locations between July 1, 2017 and March 31, 2018.
Steps taken to notify individuals of the incident	Affected individuals were notified indirectly as follows: • April 1, 2018: press release issued and preliminary notice on website; • April 2, 2018: updated website statement, including the telephone number for a call centre for customer questions; and • April 27, 2018: posted a full notice of a possible data security issue on webpages.
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 did not specifically identify any harm that might result from this incident, but its notification to affected individuals recommended they "Register for identity protection services" and "…remain vigilant by reviewing your account statements. If you believe there is an unauthorized charge on your card, please contact your card issuer immediately." In my view, a reasonable person would consider that the financial information at issue (payment card numbers and expiration dates) could be used to cause the significant harms of identity theft, fraud and financial loss.

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 did not specifically assess the likelihood that significant harm would result from this incident, but its notification to affected individuals said "… we identified the issue, took steps to contain it, and believe it no longer poses a risk to customers shopping at our stores". Further, "We want to reassure affected customers that they will not be liable for fraudulent charges that may result from this matter." In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion and installation of malware). The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud. Further, the information may have been exposed for approximately 8 months.

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.

A reasonable person would consider that the financial information at issue (payment card numbers and expiration dates) could be used to cause the significant harms of identity theft, fraud and financial loss. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion and installation of malware). The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud. Further, the information may have been exposed for approximately 8 months.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

Section 19.1(1) of the Regulation states "Where an organization is required under section 37.1 of the Act to notify an individual to whom there is a real risk of significant harm as a result of a loss of or unauthorized access to or disclosure of personal information, the notification must …be given directly to the individual". However, pursuant to section 19.1 (2), "…where an organization is required to notify an individual under section 37.1 of the Act, the notification may be given to the individual indirectly if the Commissioner determines that direct notification would be unreasonable in the circumstances."

In this case, the Organization reported that it "…is not able to determine the number of Alberta residents who may be affected by this incident…" and provided copies of the notice materials it posted on the websites of affected affiliated entities (Saks Fifth Avenue, Saks OFF STH, and Lord & Taylor). The Organization has not, however, explained exactly why "direct notification would be unreasonable in the circumstances".

Given this, and pursuant to section 37.1(2) of PIPA which states "… the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate…", **I require the Organization to report to my office within ten (10) days of the date of this decision, that affected individuals have been notified of this incident directly in accordance with the requirements outlined in the Regulation, or, why the Organization believes that direct notification is unreasonable and how steps taken to date to provide indirect notice are adequate.**

Jill Clayton
Information and Privacy Commissioner