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	Home Depot of Canada Inc. (Organization)
Decision number (file number)	P2014-ND-05 (File #P2586)
Date notice received by OIPC	February 20, 2014
Date Organization last provided information	April 02, 2014
Date of decision	July 15, 2014
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 as an extra-provincial corporation in Alberta. 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 following information was involved in this incident: • name, • address, • store location, • social insurance number (SIN), • home telephone number • work telephone number, • driver's license, and • financial information. This information is "personal information" as defined in section 1(1)(k) of PIPA and was collected in Alberta.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On December 16, 2013 an employee of the Organization notified a supervisor of the potential misuse of personal information by a co-worker. • Upon learning of the incident, the Organization investigated and also notified the United States Secret Service. • The investigation found that databases containing the information at issue had been accessed by three Human Resources (HR) employees for fraudulent purposes. • The three HR employees were arrested on allegations of unlawful use of personal information. • The Organization believes the unauthorized access may have started on or around February 7, 2011 (the date of hire for the longest serving of the three employees). • The Senior Attorney, Privacy and IT Procurement was informed of the incident on December 17, 2013. Upon learning that the personal information of Albertans was involved, the Director – Legal and Canadian Privacy Officer was notified (on February 6, 2014).
Affected individuals	• The Organization confirmed unauthorized access to and misuse of the personal information of 163 individuals in the United States. • The personal information of seven Alberta residents was contained in the database. The Organization found no evidence that this personal information was accessed or misused; however, it has not confirmed that the information was not accessed or misused.
Steps taken to reduce risk of harm to individuals	• Reported the incident to the United States Secret Service and worked with law enforcement to prosecute the HR employees. • Conducted an internal investigation. • Terminated the HR employees who accessed and misused the personal information in question. • Audited protocols and practices for employees with access to personal information. • Offered free credit monitoring offered to all potentially affected individuals. • Set up a call centre to respond to questions from affected individuals.
Steps taken to notify individuals of the incident	Notification sent by mail on February 14, 2014.

REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to those 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 investigated the incident and concluded that there was a risk of identity theft since the information is considered sensitive. In my view, the personal information involved is highly sensitive. It includes name, address, SIN and driver licence number. This information could be used to cause identity theft and fraud. In my view, 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 that there is no evidence of access to or misuse of the personal information of Alberta residents. I considered that the HR employees had access to the personal information at issue for a considerable length of time. Further, some of the personal information stored in the database was used to commit fraud. Although the Organization has no evidence that the personal information of Alberta residents was accessed and misused, neither has it confirmed that the three employees did not access the information.

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 involved is sensitive and includes name, address, SIN and driver's licence number for all affected individuals. Some personal information in the database was used to commit fraud, and three individuals are being prosecuted for this misuse of information. The three employees had access to the personal information for a considerable period of time. The Organization has not confirmed that the three employees did not access the personal information of Alberta residents. These factors contributed significantly to my decision.

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 in Alberta in a letter dated February 14, 2014, in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner