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 (Organization)
Decision number (file number)	P2015-ND-04 (File #P2860)
Date notice received by OIPC	September 15, 2014
Date Organization last provided information	October 23, 2014
Date of decision	January 14, 2015
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 and the information was collected 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 incident involved all or some of the following information: • name, • credit card number, • credit care expiration date, • cardholder verification value and service code 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	• The Organization was notified by its financial partners and law enforcement on September 2, 2014 that its payment data systems were hacked. The Organization confirmed the security incident on September 8, 2014. • The Organization reported that the incident occurred between April 2014 and Sept 8, 2014. The Organization also reported that no evidence was found to indicate that information of customers who shopped online was affected by the incident or that personal identification numbers (PINs) were compromised.
Affected individuals	At least 97,300 Albertans were affected.
Steps taken to reduce risk of harm to individuals	• The Organization initiated an investigation of the incident on September 2, 2014. • The Organization reported the incident to the United States Secret Service and Federal Trade Commission. • The Organization offered free identity protection services for a period of 12 months to customers who used credit cards in stores as of April 2014. • The Organization issued a press release and posted a notice on its website advising customers to continuously monitor their credit card transactions and credit records and report any suspicious activities to appropriate authorities. The Organization advised customers to contact TransUnion and Equifax to obtain a free copy of their credit reports.
Steps taken to notify individuals of the incident	• The Organization issued an initial press release confirming the breach on September 8, 2014. • A notice about the breach was posted on the Organization's website on September 9, 2014. • Additional notices were placed in the national edition of The Globe and Mail and La Presse on September 16, 2014. • As more information became available, the Organization issued a second press release on September 18, 2014. • The Organization provided direct notification to affected individuals via emails sent on September 21and September 22, 2014. The emails were sent to customer email addresses that the Organization could associate with payment cards used at its stores in Alberta between April and September 2014.

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 recognized that affected individuals may be at risk of harm. In my view, the personal information involved is highly sensitive. The types of harm that could result from unauthorized access to personal information in this instance are identity theft, financial loss and/or 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.	Due to the sensitivity of the personal information involved, there is a real risk of significant harm to the affected individuals. In my view, the likelihood of harm resulting from this incident is increased because the unauthorized access was due to malicious intent (hacking). Also, the Organization reported that the incident occurred in April 2014 and was only contained on September 8, 2014. The system was exposed to unauthorized individuals with malicious intent for a period of 6 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. The personal information involved sensitive credit card information and it was accessed by unauthorized individuals with malicious intent. Also, the malicious activities may have gone on for 6 months prior to the containment of the incident.

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 affected individuals directly via emails (where the Organization could associate email addresses with payment cards used at its stores) and indirectly via press releases and website notices. Where the Organization could not associate individuals' email addresses with payment cards used at its stores, I am satisfied with notifying those individuals indirectly, as direct notification would be unreasonable in that circumstance. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner