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	Polaris Industries Inc. (Organization)
File number	P2015-ND-10 (File #P2344)
Date notice received by OIPC	June 11, 2013
Date Organization last provided information	April 15, 2014
Date of decision	March 8, 2015
Summary of decision	There is 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 the state of Minnesota, U.S.A. The information at issue was collected from Alberta residents. 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 the following information about individuals who filled out dealership applications: • full name, • home address, • home telephone number, • birth date, • bank references, • banking information, • social insurance number (SIN), • criminal convictions of applicant or other managers proposed for the dealership, • civil liability for consumer fraud, unfair trade practices or similar practices of applicant or other managers proposed for the dealership, and

	• confirmation of financial resources for line of credit. This information is "personal information" as defined in section 1(1)(k) of PIPA and was collected from Alberta residents.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On May 8, 2013, the Organization discovered that applications submitted by individuals to become dealers for the Organization were accessible over the internet. • This occurred because the settings in effect did not require login credentials to access applications made. • Each application made was therefore accessible over the internet from the date it was submitted by the individual, until May 8, 2013 when the Organization discovered the issue and disabled the entire dealer application site. • The Organization's investigation determined the information was not searchable. In order for someone to access this information, it would have been necessary for them to have the exact uniform resource location (URL) where the application was stored. In other words, the applications were not "crawled" by Google or other search engines and thus should not have appeared as results in searches for the applicants' names. • The Organization's investigation revealed that with the exception of two dealer applications, all other applications affected by this incident were each accessed by only one computer which, by definition, would be the computer of the applicant. For the remaining two dealer applications, the Organization concluded that there was no indication of any inappropriate access of any application.
Affected individuals	In total, 31 Canadian applicants were impacted; 14 were Alberta residents.
Steps taken to reduce risk of harm to individuals	• The Organization disabled the entire dealer application site and will not reactivate it until all technical/security issues are resolved. • Reported the incident to the Office of the Information and Privacy Commissioner of Alberta.
Steps taken to notify individuals of the incident	Notification sent by mail on or about June 10, 2013.

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 the information was sensitive from a personal and financial perspective and if inappropriately accessed and used, the types of harm that could occur were identity theft and fraud. I agree with the Organization. In my view, the personal information involved is of high sensitivity, particularly as it includes identifiers such as birth dates and social insurance numbers. The types of harm that could result to an individual from this incident are identity theft and fraud.
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 submitted that the risk of harm occurring was very low because the personal information was difficult to access, and was not indexed by search engine crawlers. In addition, the Organization indicated it checked server logs to confirm the number of accesses made to each application. Despite repeated requests to obtain documentation about the verifications undertaken by the Organization of these server logs, I have not received such documentation. Given the information reported by the Organization, and due to the fact the information at issue could be used to cause significant harm (identity theft and fraud), I have concluded that there is a real risk of significant harm in this case. In arriving at this conclusion, I considered the circumstances of the disclosure, the sensitive nature of the personal information at issue, and the fact that some of this personal information may have been available online for an extended period of time.

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 involves sensitive identity and financial information which could be used to cause the significant harms of identity theft and fraud. The information was potentially exposed on the internet for an extended period of time, and any copies of the information obtained by third parties through the internet cannot be recovered. These factors contributed significantly to my decision. 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 the affected individuals in a letter dated June 10, 2013, in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner