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	Mars Canada Inc. (Organization)
Decision number (file number)	P2013-ND-48 (File #P2517)
Date notice received by OIPC	November 14, 2013
Date Organization last provided information	December 16, 2013
Date of decision	February 11, 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 federally incorporated. 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:
	• employees and spouses (name, address, telephone numbers, dates of birth),
	• employees:
	  ○ identification number assigned by Organization,
	  ○ social insurance number,
	  ○ gender,
	  ○ marital status,
	  ○ hire date,
	  ○ department #,
	  ○ branch #,
	  ○ account # (internal accounting software system cost centre),
	  ○ payroll administration (base hourly rate, normal hours, wage class, pay grade level, wage class, new merit

	review date, premium paid on top of base pay to production employees working on a rotating shift schedule, percentage premium paid on top of base pay related to a time-bound assignment, punctuality bonus, payroll number), and o benefits administration (plan type, federal basic life taxable benefit, compensation change reason and date, deduction for insurance premium, defined contribution pension plan contributions). This information is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On November 7, 2013, the Organization received a report from an employee that an electronic file containing personal information of 800 employees and their spouses was accessible, on a shared computer drive, to approximately 350 of the Organization's employees at a facility in Bolton, Ontario. • The Organization investigated, and found that: o during a system interface project, the electronic file was placed on the shared computer drive for temporary access by a finance employee; o the file was not encrypted and was not password protected; o the file had been accessible since July 19; o between November 1 and November 6, 2013, the file was accessed 18 times by seven unauthorized employees at the Bolton facility; o there was no evidence the file was printed, downloaded, transferred, recorded or preserved in any way. • The Organization took immediate steps to remove the electronic file from the shared computer drive.
Affected individuals	• 800 affected individuals and their spouses (unaccounted) across Canada. • Out of the 800, 25 individuals are Alberta residents.
Steps taken to reduce risk of harm to individuals	• Interviewed the seven employees who accessed the file. They reported accessing the file out of curiosity and confirmed they did not copy or download any of the

	information at issue. The employees were counseled and understand the potential consequences of sharing the information at issue with others. • Completed a forensic search of the computer disk drives of the seven employees who accessed the electronic file. • Found no evidence the electronic file was saved, printed, or mailed to any address, through the internet or any personal email accounts. • Searched the email accounts and mail files of the seven employees for any information from the electronic file and found none. • Found no evidence of the electronic file in the shared local servers or at any other locations within the Organization's computer systems. • Implemented new information and security measures for handling highly sensitive personal information. • Mandated that unsecured shared directory folders will have their content deleted at the end of each workweek. • Planning a refresher training session to ensure that all employees know their responsibilities under the Organization's Global Personal Data Privacy Policy. • Provided one year of free credit monitoring service to the affected individuals.
Steps taken to notify individuals of the incident	Notification hand delivered and/or couriered on November 13 and 14, 2013.
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 submitted that the harms that could result from the incident are fraud and identity theft. In my view, the personal data information involved is highly sensitive. It includes the employee's name, marital status, date of birth, social insurance number, and spouse's name and date of birth. The types of harm that could result from unauthorized access to this information are identity theft and fraud. In my view, these are significant harms. I find the payroll and benefits information is of low to moderate sensitivity. However, it is possible that this information could be used to cause harm in the form of damage to reputation or relationships within the Organization. These could be 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 submitted that the likelihood of fraud or identity theft resulting from the incident is low because: • the unauthorized access by the seven employees was not malicious, • the seven employees stated that they do not possess any of the information at issue, • the forensic search of the seven employees' computers and email accounts and Organization's computer systems confirmed that the electronic file was not printed, downloaded, transferred, recorded or preserved in any way. In deciding whether there is a "real risk" of significant harm in this case, I considered the following factors: • The personal data information is highly sensitive, was not encrypted and was not password protected. • The personal information was accessible to 350 employees for approximately 111 days (July 19 - November 6, 2013). • The Organization's audit software was not functional during this period. As a result, the Organization is unable to confirm there were no other unauthorized accesses.

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 information, such as social insurance numbers and date of birth. The information was not encrypted and not password protected. It was accessible to 350 employees for 111 days. The Organization is aware that seven unauthorized employees accessed the information at issue; however, as the Organization's audit software was not functional during the time the information was accessible, the Organization cannot confirm there were no other unauthorized accesses. These factors contributed significantly to my decision.

I require the Organization to notify the 25 affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified all affected individuals in a letter dated November 13, 2013, in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals in Alberta again.

Jill Clayton
Information and Privacy Commissioner