



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Co-operative Superannuation Society (CSS) Pension Plan (Organization)
Decision number (file number)	P2018-ND-017 (File #003977)
Date notice received by OIPC	October 11, 2016
Date Organization last provided information	October 11, 2016
Date of decision	January 29, 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 the individuals pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA “organization”	The Organization is an “organization” as defined in section 1(1)(i) of PIPA. The incident occurred in Alberta.
Section 1(1)(k) of PIPA “personal information”	The incident involved the following information: <ul style="list-style-type: none">• name,• address,• email address,• date of birth,• Social Insurance Number (SIN), and• signature. <p>This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA.</p>
DESCRIPTION OF INCIDENT	
<input checked="" type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">• Sometime between October 5 and 6, 2016, a rental vehicle was broken into and two cardboard boxes containing paper forms with various levels of personal information were stolen as well as microphone equipment.

	<ul style="list-style-type: none"> • The incident was discovered on October 6, 2016 when the rear hatch of the vehicle was opened and it was noticed that items were missing. • The boxes were recovered later that same morning. The Organization reported that “Upon examining the boxes, the forms with the personal information were intact and undisturbed”.
Affected individuals	The incident affected 24 individuals.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Reported incident to law enforcement on October 6, 2016. • Offered one year of credit monitoring and identity protection to the affected individuals. • Taking steps to implement policies to remove personal information from vehicles before leaving them unattended and to remove identity information from forms.
Steps taken to notify individuals of the incident	Affected individuals were notified by email sent the week of October 11, 2016.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
<p>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.</p>	<p>The Organization identified the possible harms that might result from this incident as “Identity theft and/or fraud”.</p> <p>I agree with the Organization. The identity information at issue could be used for identity theft and fraud. In addition, email addresses could be used for phishing. These are all significant harms.</p>
<p>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.</p>	<p>The Organization reported that the personal information was recovered and “the forms with the personal information were intact and undisturbed. The motivation [sic] of the individuals [sic] who broke into the vehicle appears to be theft of equipment and not data. Risk of harm assessed [sic] to be low.”</p> <p>The Organization also noted that “The persons who broke into the vehicle could have viewed and/or recorded personal information ... The information was exposed for possibly up to about 12 hours.”</p>

	<p>In my view, there is a real risk of significant harm in this case. The incident resulted from malicious intent (vehicle break-in and theft). Although the information was recovered and appeared undisturbed, the information was out of the Organization’s control for 12 hours and could have been viewed and/or recorded. The Organization can only speculate that the thieves were motivated to steal equipment not information.</p>
--	---

DECISION UNDER SECTION 37.1(1) OF PIPA

Given the information reported by the Organization, I have decided that there is a real risk of significant harm in this case.

The identity information at issue could be used for identity theft and fraud. In addition, email addresses could be used for phishing. These are all significant harms. The incident resulted from malicious intent (vehicle break-in and theft). Although the information was recovered and appeared undisturbed, the information was out of the Organization’s control for 12 hours and could have been viewed and/or recorded. The Organization can only speculate that the thieves were motivated to steal equipment not information.

The Organization is required to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand affected individuals were notified by email sent the week of October 11, 2016. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner