



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	AppCarouselDirect Inc. (Organization)
Decision number (file number)	P2021-ND-052 (File #013281)
Date notice received by OIPC	May 13, 2019
Date Organization last provided information	May 13, 2019
Date of decision	March 2, 2021
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 whose personal information was collected in Alberta, pursuant to section 37.1 of the <i>Personal Information Protection Act</i> (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA “organization”	The Organization operates in Alberta and is an “organization” as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA “personal information”	<p>The incident involved the following information:</p> <ul style="list-style-type: none">• name,• home address,• partial social insurance number (last three digits),• salary information, and• income tax information. <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 type="checkbox"/> loss <input checked="" type="checkbox"/> unauthorized access <input type="checkbox"/> unauthorized disclosure	
Description of incident	<ul style="list-style-type: none">• The Organization retains a third party service provider, TSGI Corporation (TSGI), to process and analyze tax credits.

	<ul style="list-style-type: none"> • TSGI advised the Organization that a (now) former employee of TSGI improperly accessed and collected data, some of which contained confidential information about the Organization’s current and former employees. • The breach occurred between January 28, 2019 and February 20, 2019. • The Organization understands the breach was discovered by TSGI on or about February 25, 2019. • The Organization had concluded its contractual arrangement with TSGI prior to the breach; however, TSGI retained the personal information in accordance with the terms of a Mutual Non-Disclosure Agreement and legislative records retention requirements.
Affected individuals	The incident affected 87 individuals, of which 81 had their information collected in Alberta.
Steps taken to reduce risk of harm to individuals	<p>The Organization:</p> <ul style="list-style-type: none"> • Notified affected current and former employees. <p>The Organization reported that TSGI:</p> <ul style="list-style-type: none"> • Offered affected individuals identity theft and credit monitoring solutions free of charge for 12 months. • Changed passwords on systems, devices and applications. • Shut down any remote access capability. • Installed additional security and monitoring software. • Is investigating the scope of the breach. • Engaged third-party forensic consultants. • Notified local police service and privacy regulators.
Steps taken to notify individuals of the incident	Affected individuals (current and former employees) were notified by letter on March 22, 2019.
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.	<p>The Organization reported that it “...has no evidence of any actual or attempted use or misuse of the improperly accessed information. However, based on the type of information accessed there is the potential for fraud or identity theft and negative effects on the affected individuals' credit records.”</p> <p>The Organization also said “However, ... although the information affected by the breach could potentially be used for purposes such as identity theft or fraud, absent full social insurance [sic] numbers, which were not accessed in the breach, it is unlikely that the information could be used for such purposes.”</p>

	<p>In my view, a reasonable person would consider that the contact information, in combination with partial identity, tax and employment information could be used to cause the significant harms of identity theft and fraud.</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 its assessment is...</p> <p><i>... that there is a medium likelihood of harm resulting from the breach.</i></p> <p><i>As it is currently unknown what, if anything, was done with the improperly accessed personal information it cannot be determined who, aside from the former TSGI employee, obtained or could have obtained access to the information or whether there was any malicious intent or purpose associated with the breach.</i></p> <p>In my view, a reasonable person would consider that the likelihood of identity theft and fraud resulting from this incident is increased because it resulted from deliberate, malicious action (improperly accessed). The information was exposed for almost a month. As well, there is no evidence the information was not further disseminated or disclosed.</p>
<p>DECISION UNDER SECTION 37.1(1) OF PIPA</p>	
<p>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.</p> <p>A reasonable person would consider that the contact information, in combination with partial identity, tax and employment information could be used to cause the significant harms of identity theft and fraud.</p> <p>The likelihood of identity theft and fraud resulting from this incident is increased because it resulted from deliberate, malicious action (improperly accessed). The information was exposed for almost a month. As well, there is no evidence the information was not further disseminated or disclosed.</p> <p>I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> (Regulation).</p> <p>I understand that affected individuals were notified by letter on March 22, 2019. The Organization is not required to notify the affected individuals again.</p>	

Jill Clayton
Information and Privacy Commissioner