



**PERSONAL INFORMATION PROTECTION ACT**  
**Breach Notification Decision**

<b>Organization providing notice under section 34.1 of PIPA</b>	Ericksen M-B Ltd. (o/a Mercedes-Benz Heritage Valley) (Organization)
<b>Decision number (file number)</b>	P2017-ND-153 (File #006973)
<b>Date notice received by OIPC</b>	October 19, 2017
<b>Date Organization last provided information</b>	November 16, 2017
<b>Date of decision</b>	November 22, 2017
<b>Summary of decision</b>	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 <i>Personal Information Protection Act</i> (PIPA).
<b>JURISDICTION</b>	
<b>Section 1(1)(i) of PIPA "organization"</b>	The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
<b>Section 1(1)(k) of PIPA "personal information"</b>	<p>The Organization reported the information at issue includes:</p> <ul style="list-style-type: none"><li>• "vehicle information (VIN, Model, Model 2, year) about vehicles that have been in for parts and service work at a ... dealership in China."</li><li>• "documented information regarding who the vehicle was sold to (Dealer number, Sales Person, Dealer, Region, Province, Customer First Name, Last Name, Customer Name, Company Name, Customer Address, Postal Code, Address 2)."</li></ul> <p>This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected at a dealership in Edmonton, Alberta.</p>
<b>DESCRIPTION OF INCIDENT</b>	
<input type="checkbox"/> loss <input type="checkbox"/> unauthorized access <input checked="" type="checkbox"/> unauthorized disclosure	

<p><b>Description of incident</b></p>	<ul style="list-style-type: none"> <li>• The information at issue makes up a spreadsheet listing of vehicles that have been tracked as being exported to China, along with the vehicle’s VIN number, and information about the individuals who initially purchased the vehicles in Canada. The Organization reported “The list outlined ... vehicles which had been tracked as being exported to China illegally”.</li> <li>• On or around March 27-31, 2017, a sales person with the Organization provided the list to a customer whose name appeared on it.</li> <li>• The Organization learned of the unauthorized disclosure of the list on September 26, 2017 when the customer made a complaint to the Office of the Information and Privacy Commissioner (OIPC).</li> <li>• The Organization initially believed only a portion of the list had been photographed from the salesperson’s screen and sent to the customer; however, when notified of the complaint made to the OIPC, the Organization learned the entire list had been emailed to the customer.</li> </ul>
<p><b>Affected individuals</b></p>	<p>The incident affected seventy (70) Alberta residents.</p>
<p><b>Steps taken to reduce risk of harm to individuals</b></p>	<ul style="list-style-type: none"> <li>• The Organization has made repeated attempts to send the complainant a letter asking him to destroy/delete the file from his computer and destroy any copies in his possession. On one occasion, the complainant refused to accept the letter from the delivery person. The Organization has not confirmed that the complainant has received the letter.</li> <li>• The Organization has reminded staff about their duty to protection confidential information.</li> </ul>
<p><b>Steps taken to notify individuals of the incident</b></p>	<p>The Organization reported that affected individuals “Will not be notified - alerting these exporters to the fact that they are on the list would tip them to the fact that we are on to their tactics and potentially cause further harm to our dealership and other dealerships.”</p>
<p><b>REAL RISK OF SIGNIFICANT HARM ANALYSIS</b></p>	
<p><b>Harm</b> 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>As noted above, the Organization reported “The list outlined ... vehicles which had been tracked as being exported to China illegally”. The Organization further reported that:</p> <ul style="list-style-type: none"> <li>• “Being included on the list, which is then distributed, could impact an individual's reputation. However, the list was sent only to someone already on the list and the information is not speculative - these vehicles have been documented as being exported. The individuals on the list have breached their agreements with EMB not to export the vehicles and have</li> </ul>

	<p>enjoyed tax free profits. The list was only ever intended for internal distribution...”.</p> <ul style="list-style-type: none"> <li>• “The only people that would care about this would be owners of dealerships that have the same level of care regarding exporting. There was no driver's licence information, SIN number, credit card information or even cell phone numbers shared. Just vehicle purchasers and their addresses.”</li> <li>• “People outside of the luxury automotive industry are likely unaware that exporting these vehicles is a violation of our agreements with our customers, and are also likely unaware of how common and profitable exporting is. An individual may even gain an increase in reputation by letting his or her friends know that they had made an enormous tax free profit by buying a vehicle in Canada and selling it in China.”</li> </ul> <p>In my view, the personal information at issue could be used to cause the harms of hurt, humiliation, and embarrassment, as well as damage to reputation. These are significant harms.</p>
<p><b>Real Risk</b> 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>In assessing the likelihood of harm resulting from this breach, the Organization reported:</p> <ul style="list-style-type: none"> <li>• “The breach that occurred was unfortunately initiated internally; whereby, an employee willfully forwarded an email that contained a spreadsheet created by [the Organization] that was not password protected or encrypted. The sheet was not prepared for public consumption, nor, was it the desire of [the Organization] to publicly shame any exporter.”</li> <li>• “The list was only ever intended for internal distribution, but an employee made a rash decision out of anger after her customer lied to her.”</li> <li>• “The list was sent to one individual who was on the list, but from that point forward there was a risk of it being forwarded further. That would be unlikely, though, as the complaint was sent to you [the OIPC] by the recipient, who presumably wouldn't then commit the same privacy violation.”</li> <li>• “There was no malicious intent to distributing the names, it was only to catch [the complainant] himself in a lie.”</li> </ul> <p>In my view, there is a real risk of significant harm in this case. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the deliberate action of an employee who provided the information at issue to an external third party.</p>

	<p>The information appears to have been exposed for approximately eight months and has not been recovered by the Organization. The Organization has not confirmed with the unauthorized recipient that the list has been destroyed and will not be further circulated.</p> <p>The unintended recipient may harbor ill-will towards the Organization given the information was disclosed to him “out of anger” and “to catch [the complainant] himself in a lie”, which may be incentive for the complainant to distribute the list further or to make it public.</p>
--	--

**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 at issue could be used to cause the significant harms of hurt, humiliation, and embarrassment, as well as damage to reputation. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the deliberate action of an employee who provided the information at issue to an external third party. The information appears to have been exposed for approximately eight months and has not been recovered by the Organization. The Organization has not confirmed with the unauthorized recipient that the list has been destroyed and will not be further circulated. The unintended recipient may harbor ill-will towards the Organization given the information was disclosed to him “out of anger” and “to catch [the complainant] himself in a lie”, which may be incentive for the complainant to distribute the list further or to make it public.

I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation), and confirm to me within 10 days of the date of this decision that it has done so.

As noted above, the Organization is concerned that “alerting these exporters to the fact that they are on the list would tip them to the fact that we are on to their tactics and potentially cause further harm to our dealership and other dealerships.” However, I note that when making a decision under section 37.1 of PIPA as to whether or not I will require an Organization to notify individuals affected by an incident reported to me under section 34.1, the only consideration is harm to the individual(s).

Jill Clayton  
Information and Privacy Commissioner