



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Keegan Holdings Ltd. D/B/A Bath Fitter (Organization)
Decision number (file number)	P2018-ND-004 (File #006173)
Date notice received by OIPC	August 1, 2017
Date Organization last provided information	September 18, 2017
Date of decision	January 3, 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 56 of PIPA “non-profit organization”	The Organization is incorporated in Alberta and is an “organization” as defined in section 1(1)(i)(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,• address,• date of birth,• drivers licence number, and• void cheque. <p>The information above is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA. The information was collected in Alberta.</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">• On March 24, 2017, the Organization contacted a client to request he submit a Financial Deferred Payment Application, and the client informed the Organization he had personally delivered the application, as well as a void cheque, to the Organization’s office on March 6, 2017.

	<ul style="list-style-type: none"> • The Organization confirmed it received the documents on March 6, 2017, but, after searching, was unable to find them. • The Organization surmised that the application and cheque were placed in the secure “in-bin” of an employee who was assisting the client and his wife. The employee was away the week of March 6, 2017 and did not return until the week of March 13, 2017. Shortly thereafter, the employee’s employment with the Organization ceased. • The Organization speculates that the employee inadvertently took the documents when the employee left the Organization. However, the (now former) employee denies taking the documents. • The Organization believes if the former employee had taken the documents, the documents would likely have been destroyed. If the documents were not taken by the former employee, the Organization believes they would have been shredded.
Affected individuals	The incident affected 2 individuals who are residents of Alberta.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Offered to pay for a year of credit monitoring for the affected individuals and to absorb any costs associated with closing the bank account or replacing driver’s licences. • Implemented an online application. • Removed “in-bins” and implemented new measures to secure daily correspondence. • Commenced developing an internal privacy policy to be distributed to current and future staff members.
Steps taken to notify individuals of the incident	The Organization discovered the loss of the documents during a conversation on March 24, 2017 with one of the affected individuals. A complaint about the incident was subsequently filed by the affected individuals with the Office of the Information and Privacy Commissioner. The Organization wrote to the affected individuals on September 15, 2017 to formally notify them of the incident.
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 reported that the types of harms that could occur to the affected individuals as a result of the breach were “possible identity theft” with respect to each individual’s date of birth and drivers licence, and “financial implication” with respect to the void cheque.</p> <p>In my view, the personal information involved in this incident could be used to cause the harms of identity theft, fraud, financial loss and negative effects on credit record. These are all significant harms.</p>

<p>Real Risk</p> <p>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 it believes the likelihood of harm in this case is “very low”. It stated that it believes the information was inadvertently removed from its premises by the former employee, and, given the character of the former employee, the Organization is confident the documents would have been destroyed. The Organization also said “Alternatively, if the information was shredded in our office, the risk is non-existent. There is no evidence of malicious intent, and no evidence that a third party ‘stole’ the information for the purpose of victimizing the [affected individuals]. There have been no break-ins or any ‘data breaches’ at [the Organization’s] office. The loss of the information took place approximately 6 months ago, and we are not aware of its having been used by third parties. During that 6 month period the [affected individuals] have had ample opportunity to change all account and DL numbers so as to render the missing information harmless.”</p> <p>In my view, there is a real risk of significant harm in this case. Although the Organization believes the documents were inadvertently removed by the now former employee, and that the former employee would not misuse the personal information in any way to cause harm to the affected individuals, it has no evidence to support its belief. In fact, it reported that when questioned about the documents, the former employee advised the Organization they did not take or have the documents. The Organization also cannot confirm that if the documents were not accidentally removed by the former employee, they were mixed with intra-office paperwork ready for disposal and shredded by the Organization. In light of this, the Organization cannot definitively say what happened to the documents after it received them on March 6, 2017. The fact that some time has elapsed and no harm is known to have occurred does not negate the risk that it still could occur.</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 involved in this incident could be used to cause the significant harms of identity theft, fraud, financial loss and negative effects on credit record. Although the Organization believes the documents were inadvertently removed by the now former employee, and that the former employee would not misuse the personal information in any way to cause harm to the affected individuals, it has no evidence to support its belief. In fact, it reported that when questioned about the documents, the former employee advised the Organization they did not take or have the documents. The Organization also cannot confirm that if the documents were not accidentally removed by the former employee, they were mixed with intra-office paperwork ready for disposal and shredded by the Organization. In light of this, the Organization cannot definitively say what happened to the documents after it received them on March 6, 2017. The fact that some time has elapsed and no harm is known to have occurred does not negate the risk that it still could occur.

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

I understand the Organization notified the affected individuals by letter on September 15, 2017. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner