



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Johnston Ming Manning LLP and Johnston Ming Manning (Innisfail) LLP (the Organizations)
Decision number (file number)	P2016-ND-37 (File #002777)
Date notice received by OIPC	April 11, 2016
Date Organization last provided information	May 19, 2016
Date of decision	July 22, 2016
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 <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.
Section 1(1)(k) of PIPA “personal information”	The incident involved the following information: <ul style="list-style-type: none">• client and third party names,• copies of identification,• copies of financial, employment and/or tax information,• copies of medical/health information or description of medical/other health concerns,• information about legal matters, and in particular, family law disputes,• correspondence with clients, or third parties,• copies of court documents and in some cases, drafts thereof, and• legal documents (such as Wills, Powers of Attorney, Personal Directives, Separation Agreements, land sale documents).

	This information is about identifiable individuals and is “personal information” as defined in section 1(1)(k) of PIPA.
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 22, 2016, a vehicle belonging to an associate of the Organizations was stolen while the keys were in the ignition. • A USB memory stick, with the information at issue stored on it, was attached to the keyring. • The vehicle was recovered; however, the keys and USB memory stick have not been found. • The memory stick was not password-protected nor encrypted.
Affected individuals	The Organizations believe 148 clients are affected, in addition to 100 other individuals who are parties to clients’ proceedings.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Reported the theft to the RCMP immediately upon discovery. • Notified affected individuals and recommended safeguards such as changing account numbers and passwords. • Notified the Law Society of Alberta and the Alberta Lawyers Insurance Association.
Steps taken to notify individuals of the incident	<ul style="list-style-type: none"> • All clients were notified of the incident on April 8, 2016. • On the same date, law firms representing the 100 other individuals were notified.
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 Organizations reported that “The harm that might reasonably be expected to result from the theft of the USB stick, if the information on it is accessed, used and/or disclosed by a third party, could include identity theft, fraud, financial loss, damage to reputation or relationship, loss of business, professional or employment opportunities, and negative effects on a credit record.” The Organizations also noted that “The type and severity of potential harm to the persons whose information was on the USB stick will vary, as the type of information varies” and that “most” of the documents on the USB stick are part of court records, which are public records.</p> <p>Based on the Organizations’ report of the information on the USB stick, I agree with its assessment of harm. The personal</p>

	<p>information at issue includes sensitive identity, financial, employment, medical and legal information that could be used to cause the harms of identity theft, fraud, financial loss, damage to reputation or relationship, loss of business, professional or employment opportunities, and negative effects on a credit record. These are 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 Organizations did not specifically assess the likelihood of harm resulting from this incident, but noted the thief could possibly access, use and disclose the information at issue. However, the Organizations have no knowledge that anyone has attempted to access, use or disclose the information, and does not believe the theft of the information was intentional, as it occurred in the course of a vehicle theft.</p> <p>In my view, the likelihood of harm resulting from this incident is increased because the incident resulted from deliberate action (theft of a vehicle), indicating malicious intent. The information has not been recovered. Although the Organizations do not believe the information was the target of the theft and have no knowledge of the information being used or disclosed, it is impossible to know this for sure.</p>
<p>DECISION UNDER SECTION 37.1(1) OF PIPA</p>	
<p>Based on the information provided by the Organizations 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 includes sensitive identity, financial, employment, medical and legal information that could be used to cause the harms of identity theft, fraud, financial loss, damage to reputation or relationship, loss of business, professional or employment opportunities, and negative effects on a credit record. These are significant harms. The likelihood of harm resulting from this incident is increased because the incident resulted from deliberate action (theft of a vehicle), indicating malicious intent. The information has not been recovered. Although the Organizations do not believe the information was the target of the theft and have no knowledge of the information being used or disclosed, it is impossible to know this for sure.</p> <p>I require the Organizations to notify the affected individuals in accordance with section 19.1 of the <i>Personal Information Protection Act Regulation</i> (Regulation).</p> <p>I understand the Organizations notified the affected individuals on April 8, 2016 in accordance with the Regulation. The Organizations are not required to notify the affected individuals again.</p>	

Jill Clayton
Information and Privacy Commissioner