



PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	ATB Financial (Organization)
Decision number (file number)	P2019-ND-123 (File #011400)
Date notice received by OIPC	December 20, 2018
Date Organization last provided information	December 20, 2018
Date of decision	August 2, 2019
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 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 laptop bag contained paper mortgage application documents for 7 customers and 1 team member, which included:</p> <ul style="list-style-type: none">• name,• home address,• home telephone number,• email address,• date of birth,• gender,• country of birth,• citizenship,• social insurance number (6 individuals),• drivers license number (7 individuals),• Permanent Resident Card number (1 individual),• Alberta Health Care number (1 individual),• Organization account number (2 individuals),• net worth, employment and income information (pension income, asset and liability balance). <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"> • On December 12, 2018, a team member's home was broken into and a work laptop bag was stolen. • The bag contained customer information, an Organization laptop, and some personal belongings. • The laptop was encrypted and has screen lock. The certificate for the laptop was revoked to prevent authentication or wireless connectivity to the Organization's network. • The breach was discovered the same day when the team member noticed that the items were missing.
Affected individuals	The incident affected 7 individuals.
Steps taken to reduce risk of harm to individuals	<ul style="list-style-type: none"> • Reported the theft internally to the internal Information Security and Regulatory Compliance teams, as well as police. • Immediately disabled the team member's network account. • Offering credit monitoring at no cost for 1 year.
Steps taken to notify individuals of the incident	Affected individuals were contacted by telephone and written notification was sent by December 21, 2018.
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 "Based on the personal information which was breached, we believe there is a risk of fraud and identity theft to the 7 customers whose mortgage application documents were stolen. The information provided within these files would allow someone with malicious intent to pose a real risk of significant harm to those customers. This harm may come in the form of opening of fraudulent bank accounts, loans, and credit cards. If these risks are realized these customers may also have negative effects on their credit.</p> <p>In my view, a reasonable person would consider that the contact, identity, financial and employment information at issue could be used to cause the significant harms of identity theft and fraud, and negative impacts to a credit record. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud.</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 “We believe that the likelihood that harm could occur due to the stolen laptop is low. The laptop has security safeguards in place to prevent unauthorized access to information. Once the item was reported stolen, access to the... network was revoked for the device. The likelihood of harm resulting from the stolen paper mortgage documentation is elevated as it is not clear whether the criminals are looking for items for quick financial gain or if they are into elaborate financial and/or identity crimes. To date the information contained in the mortgage application documents has not been recovered.”</p> <p>In my view, a reasonable person would consider that there is a very low risk that the information on the laptop could be used to cause significant harm due to technical safeguards in place. However, information included in the mortgage applications could be used to cause significant harm. The likelihood of harm is increased because the breach resulted from malicious action (theft). The information has not been recovered.</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 and financial information at issue, particularly in combination with identity and employment information, could be used to cause the significant harms of identity theft and fraud, and negative impacts to a credit record. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud.</p> <p>There is a very low risk that the information on the laptop could be used to cause significant harm due to technical safeguards in place. However, information included in the mortgage applications could be used to cause significant harm. The likelihood of harm is increased because the breach resulted from malicious action (theft). The information has not been recovered.</p> <p>I require the Organization 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 that affected individuals were contacted by telephone and written notification was sent by December 21, 2018. The Organization is not required to notify the affected individuals again.</p>	

Jill Clayton
Information and Privacy Commissioner