Office of the Information and
Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	ATB Financial (Organization)
Decision number (file number)	P2018-ND-135 (File # 009519)
Date notice received by OIPC	August 20, 2018
Date Organization last provided information	September 21, 2018
Date of decision	October 16, 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 those individuals pursuant to section 37.1 of the *Personal Information Protection Act* (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"	The incident involved mortgage renewal documents including all or some of the following information: • name, • telephone number, • buyer's payroll statement (name, employee number, home address, social insurance number, pay amount), and • seller's name, telephone number, property address being purchased, and property purchase price. Also at issue is a list of 45 customers and 2 Organization team members who were to be contacted. The customer information elements included on the list were: • first and last name, • city, • postal code, and • reason to be contacted.

	The team member information elements on the list included first and last name. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On August 11, 2018, an Organization team member (employee) was at a gym when her locker was broken into. The thief stole the team member's wallet and keys. • The thief used information in the wallet and keys to gain access to the team member's home where they stole a work laptop bag which contained customer information, as well as an organization-issued laptop and cell phone. • The cell phone was recovered on the side of highway 2 on August 13, 2018. • The cell phone was wiped of all data and access to the Organization's network was revoked for both devices on August 11, 2018.
Affected individuals	The incident affected 7 individuals.
Steps taken to reduce risk of harm to individuals	• Reported the matter to law enforcement and internally. • Disabled the team member's network account and wiped the mobile device of all data. • Revoked the certificate for the laptop to prevent authentication or wireless connectivity to the Organization's network. • Offering credit monitoring at no cost to the individuals for 1 year.
Steps taken to notify individuals of the incident	The Organization reported that "All 52 customers will be called to notify them of the breach indicating what personal information was disclosed. Following the call, [the Organization] will be sending the individuals written notification in compliance with section 19.1 PIPA Regulation. In addition, the two team members affected will be contacted by their manager to discuss the incident and address any concerns".

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.	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 renewal 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.* *…* *The list of 45 customers contains first and last name, city, and postal code (no house number) and the reason why the clients should be contacted. We do not believe this information poses a real risk of significant harm to those individuals as the information is not sensitive in nature and may generally be obtained through other public means e.g. telephone book. However, we are working on notifying all 45 customers.* *The 2 impacted team members only have their first and last name on the document. No other personal information is impacted. We do not believe the incident poses a real risk of significant harm to these team members but their manager will have a chat with them to inform them of the incident.* I generally agree with the Organization's assessment. The contact, identity and financial/employment information contained within the mortgage renewal documents could be used to cause the significant harms of identity theft, fraud and negative effects on a credit record. In my view, a reasonable person would not consider that the information on the list of customers and team members could be used to cause any significant harm. The Organization reported that the laptop was encrypted; therefore any personal information stored on it would not have been accessible to the thief and could not be used to cause significant harm. The Organization also reported that "The phone and contents was encrypted. [The Organization] successfully wiped everything on the phone on Aug 11 (same day the theft incident occurred)." Given this, it appears that any personal information stored on the cell phone could not have been used to cause significant harm.

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.	The Organization reported: *As a result of the breach we believe the likelihood that harm could occur is low. Both the laptop and cell phone have security safeguards in place to prevent unauthorized access to information. Once the items were reported stolen, access to the …network was revoked for those devices.* *Although it is more likely the criminals are looking for items for quick financial gain rather then elaborate financial and/or identity crimes, it is unclear what their motives or intentions might be with respect to information stolen from the team member's home. To date the information contained in the mortgage renewal documents and the contact list has not been recovered.* In my view, with respect to the mortgage renewal documents, the likelihood of harm is increased as the breach was the result of malicious intent (break-in and theft), the information was accessible (in paper format) and has not been recovered. While it may be that the criminals were looking for quick financial gain, the perpetrator(s) motives are not known. Despite the fact the breach was the result of malicious intent, the likelihood of harm with respect to information on the laptop and cell phone is reduced given the devices were encrypted.

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 in this case.

The contact, identity and financial/employment information contained within the mortgage renewal documents could be used to cause the significant harms of identity theft, fraud and negative effects on a credit record. The likelihood of significant harm resulting to these individuals is increased as the breach was the result of malicious intent (break-in and theft), the information was accessible (in paper format) and has not been recovered. While it may be that the criminals were looking for quick financial gain, the perpetrator(s) motives are not known.

The Organization reported that the laptop and cell phone were encrypted; therefore any personal information stored on these devices would not have been accessible to the thief and could not be used to cause significant harm. Similarly, in my view, a reasonable person would not consider that the information on the list of customers and team members could be used to cause any significant harm.

I require the Organization to notify the affected individuals whose personal information was included in the mortgage renewal documents, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization reported that "All 52 customers will be called to notify them of the breach [and]…will be sending the individuals written notification in compliance with section 19.1 PIPA Regulation. In addition, the two team members affected will be contacted by their manager to discuss the incident and address any concerns". **I require the Organization to confirm to my office within ten (10) days of this decision that it has notified the affected individuals whose personal information was included in the mortgage renewal documents.**

The Organization is not required to notify individuals whose personal information was included on the list of customers and team members, nor whose personal information may have been stored on the laptop or cell phone.

Jill Clayton
Information and Privacy Commissioner