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)	P2021-ND-007 (File #016819)
Date notice received by OIPC	March 4, 2020
Date Organization last provided information	January 28, 2021
Date of decision	February 16, 2021
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 whose personal information was collected in Alberta pursuant to section 37.1 of *the Personal Information Protection Act* (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 all or some of the following information: • name, • telephone number, • email addresses, • home address, • date of birth, • gender, • marital status, • social insurance number, • employment information, • financial information, • tax information, • residential purchase contract, and • signature. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The personal information was collected in Alberta.

DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On February 6, 2020, an employee's backpack was stolen as the result of a vehicle break-in. The backpack contained an encrypted laptop, tablet, and paper documents. The breach was discovered the same day. • At the time of the incident, the laptop was powered on and locked; the tablet was powered off. Access to the Organization's resources was revoked the same day for both devices. • On February 12, 2020, the backpack was returned to the employee's home. Some of the paper records, and the laptop, were recovered. The Organization also found extraneous paper records among the contents of the bag, which were not in the backpack at the time of the theft.
Affected individuals	The incident affected 6 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Laptop and tablet were full-disk encrypted. • Revoked network access certificates on stolen devices. • Disabled employee's network account. • Offered credit monitoring to impacted individuals. • Filed a police report. • Shredded the extraneous paper records after no response was received from law enforcement.
Steps taken to notify individuals of the incident	Affected individuals were notified by telephone and email by February 13, 2020.
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 reports… *…there is a risk of fraud and identity theft to impacted individuals. Personal information within the files may allow someone with malicious intent to do potential harm to the individual. This harm may come in the form of opening of fraudulent bank accounts, loans, and credit cards. If these risks are realized the individual(s) may also have negative effects on their credit.* I agree with the Organization's assessment. A reasonable person would consider the identity and financial information at issue could be used to cause the harms of identity theft, fraud, and negative effects on a credit record. Email addresses could be used

	for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are significant harms.
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 reports: *The likelihood that harm could occur due to the stolen laptop is low. The laptop and iPad have security safeguards in place to prevent unauthorized access to information. Once the items were reported stolen, access to the ATB network was revoked for the devices on February 6.* The Organization adds: *The backpack was returned to an ATB team member's doorstep on the night of February 12, 2020. Some of the paper documents recovered inside the bag were for 2 of the individuals impacted by the theft …* *When the team member's bag was returned … the laptop was in the bag however the iPad was not.* In my view, a reasonable person would consider that the likelihood of harm resulting from the theft of the laptop and tablet is decreased because of the security safeguards in place (full disk encryption) and because the laptop was returned. Despite this, the likelihood of harm resulting from the incident is increased because the personal information was compromised due to the result of malicious intent (vehicle break-in and theft). Further, personal information remains exposed as only one device, and a portion of the stolen paper records, were returned.

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.

A reasonable person would consider the identity and financial information at issue could be used to cause the harms of identity theft, fraud, and negative effects on a credit record. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are significant harms.

The likelihood of harm resulting from the theft of the laptop and tablet is decreased because of the security safeguards in place (full disk encryption) and because the laptop was returned. Despite this, the likelihood of harm resulting from the incident is increased because the personal information was compromised due to the result of malicious intent (vehicle break-in and theft). Further, while the un-returned tablet was encrypted, personal information remains exposed as only a portion of the stolen paper records were recovered.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified affected individuals by telephone and email by February 13, 2020, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner