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 Winfield Agency (Organization)
Decision number (file number)	P2019-ND-114 (File #012595)
Date notice received by OIPC	March 25, 2019
Date Organization last provided information	March 25, 2019
Date of decision	July 31, 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 *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 paper account applications, account/investment documents, cheque deposits, and account printouts. From these documents it was determined that the following information is at issue for 11 individuals: • name, • home address, • telephone number, • email address • date of birth, • gender, • social insurance number, • driver's license number • passport number, • financial information (internal account number, balance, net worth), and • employment and income information (asset and liability balance). The following information is at issue for 24 individuals:

	• name, • home address, and • financial information (internal account number, balance, external account number). In addition to the above, the incident involved cheques which were deposited into both personal and business accounts of the Organization's clients. Information on the cheques may include: • name • home address, • telephone number, • internal account number, and • external account number and transit. 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 March 8, 2019 at approximately 3:30 am the Organization experienced a break-in and a safe was stolen. • The information at issue was stored within the safe. • The safe was recovered, but was empty. None of the safe's contents have been recovered.
Affected individuals	The incident affected 93 individuals.
Steps taken to reduce risk of harm to individuals	• Contacted home branch to report the robbery. • Reported the breach to law enforcement. • Offering to meet with affected individuals in person. • Offering credit monitoring at no cost for 1 year.
Steps taken to notify individuals of the incident	The Organization reported that all affected individuals will have been notified by telephone by March 25, 2019 and letters sent by March 29, 2019.
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	The Organization reported: *Based on the personal information that was breached, we believe there is a risk of fraud and identity theft to the 11 customers whose documents were stolen. The information provided within these files would allow someone with malicious intent to pose a real risk of significant harm to*

non-trivial consequences or effects.	*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…* *24 individuals were also impacted had either their name and account number stolen or their name and balance stolen. We believe the risk of this information posing a real risk of significant harm to the individuals in the future is low as more information would be required in order to fraudulently access these individuals' accounts. Additional information will be required to access their account e.g. proper authentication, security questions or verbal password, and transactional history knowledge…* *We also believe the risk of harm to the 58 individuals who wrote the cheques to our clients is low. The cheques which were deposited had the backs stamped with the … agent's date stamp. This stamp includes the location, transit, and date which the cheque was negotiated. As the cheques have already been stamped they should not be accepted by another financial institution for negotiation…* In my view, 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.
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 "The likelihood of harm resulting from the stolen documentation is elevated. When the safe was discovered later in the day March 8th there was evidence of heat and burning both inside and out caused by the suspects when they broke into the safe. The Organization was not able to confirm if the documents were destroyed under these conditions as the documents contained in the safe have not been recovered and it is not clear whether the robbers are looking for items for quick financial gain or if they are into elaborate financial and/or identity crimes." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the breach resulted from malicious action (theft), and given the circumstances, the contents of the safe were likely the target of the theft. The information has not been recovered. While I acknowledge the Organization's assessment that some combinations of personal information elements are more likely to

	give rise to significant harm than others, all of the combinations described by the Organization could be used to cause significant harm and, given the circumstances of the breach, the likelihood is elevated.

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 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.

The likelihood of harm resulting from this incident is increased because the breach resulted from malicious action (theft), and given the circumstances, the contents of the safe were likely the target of the theft. The information has not been recovered.

While I acknowledge the Organization's assessment that some combinations of personal information elements are more likely to give rise to significant harm than others, all of the combinations described by the Organization could be used to cause significant harm and, given the circumstances of the breach, the likelihood is elevated.

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

I understand that all affected individuals were notified by telephone or letter by March 29, 2019, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner