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	Advantage Financial Services (Organization)
Decision number (file number)	P2019-ND-086 (File #008594)
Date notice received by OIPC	May 8, 2018
Date Organization last provided information	April 24, 2019
Date of decision	June 25, 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 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, • social insurance number, • financial information, • tax forms, and • account statements. 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 7, 2018, the Organization discovered that its offices had been broken into the previous night. • The Organization determined that a number of items had been stolen, including a computer.

	• The computer was password protected and the biometric facial reader was activated. There was a separate password to access the email application. • The Organization stated it was highly unlikely that any personal information was stored locally on the computer and its internal investigation of the breach did not find evidence to suggest otherwise. • The Organization reset passwords for all web applications that had access to client data and instructions were sent to the computer to erase all content should the computer ever attempt to reconnect to an internet connection.
Affected individuals	The incident potentially affected approximately 168 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Retained a cyber security firm to assist with an investigation of the incident. • Reset all passwords for all staff. • Reset passwords for online services. • Issued a kill command through the portal so as to 'wipe' any data on the device should it be accessed. • Notified law enforcement. • Changed all locks and installed an alarm and camera system. • Monitoring accounts for suspicious activity. • Notified affected individuals and offered free credit monitoring services.
Steps taken to notify individuals of the incident	Affected individuals were notified by telephone between April 12, 2018 and April 17, 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.	The Organization reported that "If the information were to be accessed, it could potentially be used for fraud, identity theft or negatively impact a customer's credit record". Further, "In the unlikely event that an unauthorized user could bypass the security measures of the device and avoid the data from being automatically "wiped", given that the information could include social insurance numbers ("SINs") and banking information and that this information could be used for fraudulent activities (including identity theft), the level of sensitivity of information should be highly sensitive." I agree with the Organization's assessment. A reasonable person would consider that the identity and financial information at issue could be used to cause the significant harms of fraud, identity theft or negatively impact a customer's credit record.

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 that "it is important to recognize that to date, [the Organization] has not identified any unusual activity on any accounts for those who could be potentially affected by the …computer theft. Neither has any [of the Organization's] client [sic] reported any suspcious [sic] activity. While there is a potential risk of harm if an unauthorized user were somehow able to gain access to the device and its contents, this is extremely unlikely." In my view, the likelihood of harm resulting from this incident is increased because it resulted from malicious intent (theft). Although, the Organization believes it is highly unlikely that any personal information was stored locally on the computer, it cannot rule out the possibility. Further, the computer was not encrypted and the information has not been recovered.

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 identity and financial information at issue could be used to cause the significant harms of fraud, identity theft or negatively impact a customer's credit record. The likelihood of harm resulting from this incident is increased because it resulted from malicious intent (theft). Although, the Organization believes it is highly unlikely that any personal information was stored locally on the computer, it cannot rule out the possibility. Further, the computer was not encrypted and the information has not been recovered.

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

I understand the Organization provided verbal notification to affected individuals between April 12, 2018 and April 17, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner