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	Shafik Hirani's Private Wealth Management Practice of Aligned Capital Partners (Organization)
Decision number (file number)	P2019-ND-096 (File #011943)
Date notice received by OIPC	February 4, 2019
Date Organization last provided information	February 4, 2019
Date of decision	June 28, 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 Organization reported the incident involved: *Email correspondence for 2 weeks prior to loss contained document attachements [sic] that if downloaded could expose client data that includes SIN, and bank account numbers. This affects 8 individuals. Others individuals captured in the email review had documents that contained account numbers, and in some cases holdings.* 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	• An employee left his cell phone at a sporting event the evening of December 9, 2018.

	• Although client information was not saved on the cell phone, email communication between clients and the employee would have been retained for what the Organization believes to be a period of less than 2 weeks. • The Organization used its email archiving system to analyze the content of all emails sent to and from the employee's email address for that period of time. Some email correspondence had attachments that contained sensitive client information; however, the Organization reported that in order to access information contained in these documents, they would have to be downloaded from the exchange server. • The loss of the cell phone was discovered by its owner on December 10, 2018.
Affected individuals	The incident affected approximately 50 individuals.
Steps taken to reduce risk of harm to individuals	• Reported incident to law enforcement. • Monitored client accounts for any unusual activity, with none noted to date. • Changed passwords for all systems accessed by the entire office were changed which included email passwords. • The Organization reported that "As part of our cybersecurity policy we advise our agents and their employees to encrypt and lock down devices with passwords. We also advise them to take steps to ensure devices are secured at all times and their whereabouts [sic] known."
Steps taken to notify individuals of the incident	The eight (8) individuals with SIN and bank account information at issue were contacted verbally and given the choice of having credit monitoring for 12 months. Individuals for whom account numbers and investment holdings were present in the attachments were advised in writing. Affected individuals were notified verbally between January 7 -9, 2019 and in writing on February 4, 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 non-trivial consequences or effects.	The Organization reported possible harms include "Potential fraud, exposure to phishing scam attempts in some situations." In my view, a reasonable person would consider that the identity and financial information at issue could be used to cause the significant harms of 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: *Client information was not stored on the cell phone. Any possible access to client information would have had to have been through access to the email account that was on the cell phone. We believe the following to be significant mitigating steps:* *1. Default settings for email retention were not changed and believed to be no more than 2 weeks.* *2. Phone was locked down by service provider within 12 hours of loss. Service provider was contacted at 8am on Dec 10, 2018 who assured assistant that his phone was locked and that any data on the phone was secured. Locking of the phone prevented any download of data or documents that would have been associated with email correspondence.* *3. Remote wipe command was sent on December 12 at 10am, and has been monitored to see if it has been triggered. This has not yet occurred which suggests the cell phone has not accessed the internet.* The Organization also said "Given the nature of the device that was lost, and the steps taken we bellieve [sic] the likelihood of harm to be very low for all 3 categories of individuals. The window of time that access to the server could potentially occur was short (less than 12 hours). Moreover, the fact that this involved the misplacement of the device, rather than a targeted attack makes likely that even if the device was obtained by an unauthorized party within the time period that it could have potentially accessed our server, the device itself, rather than information contained on our server, would be the that [sic] party's primary interest." In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is reduced because it was not cause by malicious action, such as theft, but rather misplacement of a device. However, to date, the cell phone has not been recovered, and may be in the hands of a third party. From the Organization's report, it is not clear if the phone was encrypted, or merely "locked". The information at issue may have been exposed for up to 12 hours.
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 identity theft and fraud. The likelihood of harm resulting from this incident is reduced because it was not cause by malicious action, such as theft, but rather misplacement of a device. However, to date, the cell phone has not been recovered, and may be in the hands of a third party. From the Organization's report, it is not clear if the phone was encrypted, or merely "locked". The information at issue may have been exposed for up to 12 hours.

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 affected individuals were notified verbally between January 7 -9, 2019 and in writing on February 4, 2019. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner