ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2013-ND-25

Investment Industry Regulatory Organization of Canada

June 21, 2013

(Case File #P2299)

I. Introduction

[1] Under s. 34.1 of the *Personal Information Protection Act* (PIPA), an organization having personal information under its control must, without unreasonable delay, notify me of any incident involving the loss of or unauthorized access to or disclosure of the personal information where a reasonable person would consider that there exists a real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure.

[2] On March 27, 2013, the Investment Industry Regulatory Organization of Canada (Organization) provided notice of an incident involving the loss of personal information. For the reasons that follow, I have decided that there is a real risk of significant harm to individuals as a result of the incident. I require that the Organization notify the individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[3] Section 37.1 of PIPA authorizes me to require an organization to notify individuals to whom there is a real risk of significant harm as a result of an incident. It states:

> 37.1(1) Where an organization suffers a loss of or unauthorized access to or disclosure of personal information that the organization is required to provide notice of under section 34.1, the Commissioner may require the organization to notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure

(a) in a form and manner prescribed by the regulations, and

(b) within a time period determined by the Commissioner.

(2) If the Commissioner requires an organization to notify individuals under subsection (1), the Commissioner may require the organization to satisfy any terms or conditions that the Commissioner considers appropriate in addition to the requirements under subsection (1).

(3) The Commissioner must establish an expedited process for determining whether to require an organization to notify individuals under subsection (1) in circumstances where the real risk of significant harm to an individual as a result of the loss or unauthorized access or disclosure is obvious and immediate.

(4) The Commissioner may require an organization to provide any additional information that the Commissioner considers necessary to determine whether to require the organization

(a) to notify individuals under subsection (1), or

(b) to satisfy terms and conditions under subsection (2).

(5) An organization must comply with a requirement

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), or

(c) to satisfy terms and conditions under subsection (2).

(6) The Commissioner has exclusive jurisdiction to require an organization

(a) to provide additional information under subsection (4),

(b) to notify individuals under subsection (1), and

(c) to satisfy terms and conditions under subsection (2).

(7) Nothing in this section is to be construed so as to restrict an organization's ability to notify individuals on its own initiative of the loss of or unauthorized access to or disclosure of personal information.

[4] PIPA applies to organizations, defined in section 1(1)(i) of PIPA as follows:

1(1) (i) "organization" includes

(i) a corporation,

(ii) an unincorporated association,

(iii) a trade union as defined in the *Labour Relations Code*,

(iv) a partnership as defined in the *Partnership Act*, and

(v) an individual acting in a commercial capacity,

but does not include an individual acting in a personal or domestic capacity;

[5] The Organization oversees investment dealers and trading activity on debt and equity marketplaces in Canada. The Organization is federally incorporated and registered in Alberta as an extra- provincial non-profit corporation. It is recognized under section 64 of the Alberta *Securities Act* as a self-regulatory organization.

[6] The incident involved information collected from 5 investment dealers in Alberta with respect to approximately 469 affected individuals. As part of its mandate, the Organization is responsible for monitoring compliance with securities laws and rules. The investment dealers were required to provide the information to the Organization for compliance purposes.

[7] I have jurisdiction in this matter because the Organization is an "organization" as defined in section 1(1)(i)(i) of PIPA and the information was collected in Alberta from Alberta residents.

[8] The Organization reported the incident involved the following information of affected individuals:

- name,
- address,
- date of birth,
- investment dealer and account number.

[9] For 5 affected individuals, in addition to information listed in paragraph [8], the information also included one or a combination of the following:

- social insurance number,
- identification documents (copy of driver's licence, passport or medical card),
- bank account number,
- financial information (account equity, net worth, income), or
- a copy of a cancelled cheque.

[10] The above information qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

III. Background

[11] On April 30, 2013 and May 1, 2013, my Office requested the Organization provide additional information. The additional information was provided by the Organization on May 6, 2013.

[12] The circumstances of the incident as reported to me by the Organization are as follows:

- In February 2013, an Organization examiner accidently lost a portable device containing the personal information. The personal information was collected for the purpose of compliance examinations.
- The portable device was not encrypted.
- The portable device has not been recovered.
- The Organization retained an independent third party to assist with the forensic investigation.
- The Organization has undertaken a review of its security and business policies and protocols as a result of this incident.
- The Organization notified affected individuals by mail of the incident on April 12, 2013.
- The Organization set up a call center to address any questions from affected individuals.
- For all affected individuals, the Organization placed a six year alert service on credit files of affected individuals at Equifax Canada and TransUnion Canada. It also offered a one year credit monitoring service by Equifax Canada.
- For the 5 affected individuals described in paragraph [9], the Organization also offered a one year credit monitoring service by TransUnion Canada.
- The alert service and credit monitoring service were provided or offered by the Organization at no cost to affected individuals.

IV. Is there a real risk of significant harm to individuals as a result of the incident?

[13] In considering whether to require the Organization to notify the affected individuals, I am mindful of PIPA's purpose, legislative principles, and the relevant circumstances surrounding the reported incident.

[14] Pursuant to section 37.1 of PIPA, I have the power to require the Organization to "notify individuals to whom there is a real risk of significant harm as a result of the loss or unauthorized access or disclosure." In determining whether or not to require the Organization to notify the affected individuals, I must consider if there is a "real risk of significant harm" to the affected individuals as a result of the incident.

[15] In order for me to require that the Organization notify the affected individuals, there must be some harm – some damage or detriment or injury – that could be caused to

those 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.

[16] The Organization reported the incident posed a risk of fraud or phishing with respect to the affected individuals due to the sensitivity and volume of the personal information involved.

[17] The personal information at issue is of high sensitivity. It includes the name, contact information, and dates of birth of affected individuals. For 5 affected individuals, their social insurance number or copies of identification documents and financial or banking information were also involved. The type of harm that could result from unauthorized access to the personal information in this instance is identity theft, fraud or phishing. In my view, these are significant harms.

[18] In order for me to require the Organization to notify the affected individuals, there must also be a "real risk" of significant harm to the affected individuals as a result of the incident. This standard does not require that significant harm will certainly result from the incident, but the likelihood that it 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.

[19] Based on the above and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals as a result of this incident. The personal information is highly sensitive. While the circumstances surrounding the loss did not involve nefarious intent, the personal information has not been recovered. The personal information was not encrypted. These factors contributed to my decision that there is a real risk of significant harm to the affected individuals as a result of this incident.

V. Decision

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

[21] I understand that the Organization has notified the affected individuals in accordance with the Regulation in letters sent out on April 12, 2013. I will, therefore, not require the Organization to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner