ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-18

Combined Insurance Company of America

July 26, 2012

(Case File #P2117)

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 May 30, 2012, Combined Insurance Company of America (the "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 incident involved a branch office of the Organization located in Medicine Hat, Alberta. The Organization is licensed as an insurance company operating in Alberta pursuant to the Alberta *Insurance Act*.

[6] The Organization reported the incident involved renewal payments (the "Payments") of nine customers (the "Affected Individuals") and the following information:

- eight personal cheques.
- one Affected Individual's credit card number with expiry date.

The Organization does not have a copy of the personal cheques involved and therefore did not identify what personal information appeared on the cheques. Generally, personal cheques have an individual's name, bank account number, bank branch number and a signature. Personal cheques may also contain an address or phone number.

[7] I have jurisdiction in this matter because the Organization is an "organization" as defined in section 1(1)(i) of PIPA and the information qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

III. Background

[8] On June 11, 2012, my Office requested the Organization provide additional information. The additional information was provided by the Organization on June 18, 2012.

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

- A sales representative visited the homes of the Affected Individuals between October 31, 2011, and November 4, 2011, to renew policies and collect the Payments.
- Around November 14, 2011, the sales representative believes a sealed envelope containing the Payments was lost while transporting it to her vehicle.
- The incident was reported to her manager. The police were also notified.

- During the week of November 14, 2011, the sales representative attended on the homes of the Affected Individuals and verbally notified them of the incident.
- Two of the Affected Individuals are seniors. The sales representative assisted them with placing a stop payment on their cheques.
- The head office of the Organization was informed of the incident January 31, 2012. An investigation was conducted.
- The Payments have not been recovered.

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

[10] 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.

[11] 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.

[12] 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.

[13] The personal information at issue is of moderate to high sensitivity. The type of harm that could result from the loss of the personal information in this instance is identity theft or financial fraud. In my view, this is a significant harm.

[14] 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.

[15] The Organization reported that following an investigation of the incident, it concluded that the loss was not a material breach resulting in a real risk of harm to any of the Affected Individuals. The Organization has not received any reports with respect to any fraudulent activity as a result of the incident. The Organization noted that the Affected Individuals were notified shortly after discovery of the incident. The Affected Individuals were advised by the Organization to cancel the Payments if made by cheque or cancel the credit card payment.

[16] In deciding whether there exists a "real risk" of significant harm in this case to the Affected Individuals, I considered the following factors:

- The Payments were not recovered.
- The incident was the result of human error.
- While the Organization cannot confirm what personal information was contained on each of the eight cheques, the presence of a name and signature in combination with the bank account and location pose a real risk for financial fraud or identity theft. A credit card number with expiry date of one Affected Individual was also included in the Payments.
- The Organization indicated that two of the customers were senior citizens who are, in my view, a vulnerable group with respect to financial fraud or identity theft.

[17] Based on the information reported to me by the Organization, I have decided that there is a real risk of significant harm to the Affected Individuals as a result of this incident.

V. Decision

[18] I require the Organization to notify the Affected Individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (the "Regulation").

[19] I understand the Organization's sales representative provided direct, verbal notification to the Affected Individuals during the week of November 14, 2011, that was in accordance with the requirements of the Regulation. Therefore, I will not require the Organization to notify the Affected Individuals again.

Jill Clayton
Information and Privacy Commissioner