

ALBERTA
**OFFICE OF THE INFORMATION AND
PRIVACY COMMISSIONER**

P2012-ND-12

State Farm Mutual Automobile Insurance Company

June 11, 2012

Case File #P2101

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 April 25, 2012, State Farm Mutual Automobile Insurance Company (the “Organization”) provided notice of an incident involving the unauthorized disclosure of personal information. For the reasons that follow, I have decided that there is a real risk of significant harm to the individual as a result of the incident. I require that the Organization notify the individual 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 is an extra-provincial federally incorporated corporation carrying on business in Alberta. The incident occurred in Ontario involving a service provider retained by the Organization.

[6] The affected individual is a retiree of the Organization and a resident of Alberta (the “Retiree”). The incident involved the disclosure of a Canada Revenue Agency T1198 form entitled “Statement of Qualifying Retroactive Lump Sum Payments” (the “Statement”) that contained the following information of the Retiree:

- name,
- social insurance number, and
- payment information, including principal and interest amounts, reason for payment, and year of payment.

[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 May 4, 2012, my Office requested the Organization provide additional information. The additional information was provided by the Organization between May 4, 2012, and May 29, 2012.

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

- A service provider retained by the Organization to perform pension administration services (the “Service Provider”) was involved in the incident.
- The Service Provider notified the Organization that it mailed the Retiree’s Statement to another individual in error.
- The error occurred with respect to the Statement mailed on February 24, 2012.

- The Service Provider cannot accurately identify the individual who may have received the Retiree’s Statement. The Service Provider has been unable to recover the Statement.
- On March 1, 2012, the Service Provider provided the Retiree with a new Statement.
- On March 19, 2012, the Service Provider sent the Retiree a letter with respect to the incident.
- The Service Provider offered to protect the Retiree from any losses or expenses incurred as a result of the incident and offered credit monitoring services for one year.

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 individual, 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 individual, I must consider if there is a “real risk of significant harm” to the affected individual as a result of the incident.

[12] In order for me to require that the Organization notify the affected individual, there must be some harm – some damage or detriment or injury – that could be caused to the affected individual 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] I do not consider the payment information on the Statement to be sensitive. Disclosure of this information cannot reasonably result in significant harm in this instance. However, the name and the social insurance number of the Retiree are highly sensitive personal information. The type of harm that could result from unauthorized disclosure to this personal information in this instance is identity theft or fraud. In my view, this is a significant harm.

[14] In order for me to require the Organization to notify the affected individual, there must also be a “real risk” of significant harm to the affected individual 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 has indicated that the Retiree’s personal information has not been misused. The Service Provider indicated that the likelihood of any issue arising from the incident is very low.

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

- The incident was the result of a mailing error and not associated with malicious intent.
- The Service Provider is unable to accurately identify where the Statement was sent.
- The Statement has not been recovered.
- The name and social insurance number of the Retiree could be used for identity theft or fraud.

[17] In Breach Decision 2012-ND-06, an error in printing tax reporting statements resulted in the unauthorized disclosure of personal information, including the name and social insurance number of affected individuals. I decided there was a real risk of significant harm to the affected individuals because a number of the statements were not recovered, the sensitivity of the information, and the number of affected individuals.

[18] Based on the information reported to me by the Organization and considering that the Retiree Statement involved sensitive information that was not recovered, I have decided that there is a real risk of significant harm to the Retiree 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 that the Service Provider notified the Retiree in accordance with the Regulation in a letter sent on April 24, 2012. Therefore, I will not require the Organization to notify the Retiree again.

Jill Clayton
Information and Privacy Commissioner