**ALBERTA**

**OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER**

**P2010-ND-001**

**THE KNIGHTS OF COLUMBUS CHARITABLE FOUNDATION**

August 9, 2010

(Case File #P1631)

## I. Introduction

[1] On July 8, 2010, I received a report from The Knights of Columbus of an incident involving the loss of, and possible unauthorized access to and disclosure of, personal information of individuals in Alberta. Based on the information reported to me, I have decided that there is a real risk of significant harm to those individuals as a result of the incident, and therefore I require that The Knights of Columbus notify those individuals to whom there is a risk of harm.

## II. Jurisdiction

[2] 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.

[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 signification 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] The Knights of Columbus reported that the information at issue in this incident consists of "underwriting files and additional documents containing one or more of the following – name, address, Social Security number, financial account number, drivers' license number, medical and/or other personal information of individuals …".

[5] This is information about identifiable individuals and so qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

[6] The Knights of Columbus also reported that it is "a nonprofit fraternal benefit society incorporated in the [United States (US)] and licensed with the Alberta Superintendent of Insurance. It sells insurance on a nonprofit basis and has no office or permanent establishment in Canada."

[7] Pursuant to sections 56(2) and (3), PIPA does not apply to a "non-profit organization" except in the case of personal information that is collected, used or disclosed in connection with any commercial activity. "Non-profit organization" is defined in section 56(1)(b)(i) of PIPA to mean "… an organization that is incorporated under the *Societies Act* or the *Agricultural Societies Act* or that is registered under Part 9 of the *Companies Act* …".

[8] The Knights of Columbus operates on a non-profit basis, but is not incorporated under the *Societies Act* or the *Agricultural Societies Act*, nor is it registered under Part 9 of the *Companies Act*. Therefore, The Knights of Columbus does not qualify as a "non-profit organization" for purposes of PIPA.

[9] The Knights of Columbus is, however, licensed with the Alberta Superintendent of Insurance pursuant to section 19 of the *Insurance Act.* The Knights of Columbus also reported that it is "incorporated in the US."

[10] 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;

[11] In Order P2005-005 (para. 19), I adopted a broad definition of the meaning of "corporation". The Knights of Columbus has reported that it is "incorporated in the US" and that it is licensed with the Alberta Superintendent of Insurance; given this information, I find that The Knights of Columbus is an "organization" that is subject to PIPA, and the provisions of PIPA apply fully to the Knights of Columbus's collection, use and disclosure of the personal information of Albertans. Therefore, despite the fact the breach incident in question occurred in the US, I have jurisdiction in this matter because the personal information involved includes that of a number of Albertans and was collected by an organization licensed to operate in Alberta.

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

## III. Background

[13] On July 8, 2010, I received a written report from The Knights of Columbus describing an incident involving the loss of, and possible unauthorized access to and disclosure of, personal information.

[14] On July 19, 2010, my Office contacted The Knights of Columbus by telephone to request that it provide additional information concerning the incident, in order for me to determine whether to require The Knights of Columbus to notify individuals under subsection 37.1(1) of PIPA. Additional information – including an update on the status of the organization's investigation – was also requested via emails sent between July 20, 2010 and August 4, 2010.

[15] In summary, the circumstances of the incident reported to me are as follows:

- On or about June 15, 2010, The Knights of Columbus was notified that a small number of its underwriting files and some additional documents containing personal information had been found outdoors near its headquarters in New Haven, Connecticut.
- Based on dates printed on some of the documents, it was determined that the incident must have occurred within a few days of The Knights of Columbus being notified.
- The Knights of Columbus immediately took steps to recover the documents, protect its systems and operations, and determine the cause of the incident. The files and a significant number of documents were recovered.
- While investigating the incident, The Knights of Columbus learned that other underwriting files were not in their designated locations and may be missing from its premises.
- The Knights of Columbus is investigating to determine the cause of the incident and circumstances surrounding the other missing files. However, at this time, it is not known if the files were inadvertently disposed of, whether as the result of employee carelessness or an intentional action intended to cause harm. The whereabouts of the additional files, and cause of their disappearance, is not known.
- The total number of affected individuals is 305, including 9 Alberta residents. The Knights of Columbus reported it would be notifying all affected individuals, and provided a draft of its notification letter.
- The Knights of Columbus has received no information indicating the information at issue has been improperly utilized and does not believe there to be a real risk of harm to the affected individuals.
- The Knights of Columbus is re-examining its current data privacy and security policies and procedures to find ways to reduce the risk of future data breaches.

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

[16] Pursuant to section 37.1 of PIPA, I have the power to require The Knights of Columbus 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 Knights of Columbus to notify individuals, I must consider whether there exists a "real risk of significant harm" to individuals as a result of the incident.

[17] In order for me to require that The Knights of Columbus notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to individuals as a result of the incident; moreover, that harm must be "significant" – it must be important, meaningful, and with non-trivial consequences or effects.

[18] In this case, the personal information at issue is of moderate to high sensitivity as it includes names, addresses, Social Security numbers, financial account numbers, drivers' license numbers, medical and/or other personal information of individuals.

[19] This is information that could be used to cause significant financial harm to individuals, and provides comprehensive individual profiles that could be used for identity theft and/or fraud.

[20] In order for me to require The Knights of Columbus to notify individuals, however, there must also be a "real risk" of harm to individuals as a result of the incident. This standard does not require that harm will certainly result from the incident, but the likelihood that it will result must be more than mere speculation or conjecture. Further, there must be a cause and effect relationship between the incident and the possible harm.

[21] I note that the length of time the information was exposed in this case was relatively short; that is, The Knights of Columbus determined that the incident must have occurred within a few days of the organization being notified and, upon being notified, took steps to immediately recover the information, and believes most of it was recovered. The Knights of Columbus also reported that it does not believe there to be a real risk of harm to the affected individuals. However, at this time, and despite ongoing investigation, the cause of the incident is still unknown. The whereabouts of the additional files is also unknown, as is the cause of their disappearance, and the length of time they have been missing.

[22] Given the sensitivity of the information at issue, and considering that it is not known whether the files were inadvertently disposed of by a careless employee, or alternatively, accessed by someone with intent to cause harm, I believe there to be a real risk of harm in this case.

## V. Decision

[23] Based on the information reported to me by The Knights of Columbus, I have concluded there is a real risk of significant harm to individuals as a result of this incident, and I require The Knights of Columbus to notify individuals in Alberta.

[24] I understand The Knights of Columbus did notify Canadian residents on its own initiative, by letter dated July 15, 2010, and two additional Alberta residents, by letter dated July 23, 2010.

Frank Work, Q.C.
Information and Privacy Commissioner