ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-026

CANADIAN STANDARDS ASSOCIATION

June 29, 2011

(Case File #P1866)

I. Introduction

[1] On April 28, 2011, I received a report from Canadian Standards Association ("CSA") of an incident involving the unauthorized access to personal information. Based on the information reported to me, I have decided that there is a real risk of significant harm to individuals as a result of the incident, and therefore I require that CSA notify the individuals to whom there is a real risk of significant 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 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] Sections 56(2) and (3) of PIPA specify that the Act does not apply to a "non-profit organization" except in cases where personal information is collected, used or disclosed in connection with a commercial activity. However, a "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.*

[5] Although CSA is a non-profit organization, it is a federally incorporated non-profit association under Part 2 of the *Canada Incorporations Act* that is registered in

Alberta as an extra-provincial, non-profit corporation. Therefore, CSA is not considered a "non-profit organization" for the purposes of PIPA; rather, it is considered an "organization".

[6] 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;

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

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

III. Background

[9] On April 26, 2011, I received a written report from CSA describing an incident involving the unauthorized access to personal information.

[10] The circumstances of the incident reported to me are as follows:

- On March 16, 2011 CSA's IT department discovered a new generation Qakbot virus on its network and contacted its anti-virus supplier to request an update patch.

- By March 18, 2011, the anti-virus supplier had created a new patch which was promptly installed by CSA. By March 20, 2011, CSA had blocked all of the IP addresses where the compromised data was believed to have been transferred.

- CSA performed a detailed third party forensic audit on its system to determine the extent of the breach.

- CSA determined that only the personal information entered by employees had been affected by the virus – CSA's own databases of both client and employee information were not affected.
    - Employee computers in CSA offices in Alberta, British Columbia, Ontario, Quebec, and various locations in the United States, Mexico and India were affected by the virus.
    - 45 employees in Alberta were affected.

- The virus accessed information that the employees themselves had entered when they used their work computers to access the Internet, including if they accessed the computer for personal reasons. CSA explained the following:
    - The virus operated by capturing historical pre-populated internet form data that was stored on the computer's cache. For example, if an employee had chosen to select a "remember me" type feature that permitted a website to pre-populate form information such as login ids, passwords or account numbers, the virus targeted that type of cached information.
    - The virus also captured live key stroke data entered during the time the virus was active. CSA's forensic investigation determined the virus focussed on capturing and transmitting personal account information entered into internet based forms. Other types of information entered while the virus was active were not accessed.

- During its investigation, CSA conducted a random sampling of employee computers to determine what sort of personal information might be at risk. CSA determined from its random sampling that the credit card and personal website login information of at least one employee had been compromised. CSA states that similar information of other employees may have been accessed.

- CSA provided immediate verbal notification to the employee whose personal information had conclusively been accessed. CSA notified all of its employees via email by April 5, 2011 and included advice to assist employees in protecting themselves against identity theft.

- CSA centrally manages its data to receive frequent security patches and its anti-virus definitions are updated daily. CSA had previously applied a patch for the Qakbot virus, but was attacked by a new generation of the virus before a new patch had been created. CSA's anti-virus provider quickly created a patch for the new generation of the virus when it was discovered and CSA added the patch as quickly as it could.

- CSA indicated the Qakbot virus has been associated with organized crime and deliberate theft of information

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

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

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

[13] In this case, the personal information at issue is of high sensitivity as it includes a variety of CSA employees' personal information such as website login and passwords, credit card information and as any other personal information employees may have entered online while the Qakbot virus was active.

[14] CSA also noted that the type of harm that could result from the unauthorized access to or disclosure of this information is identity theft, which, in my view, is a significant harm.

[15] In order for me to require CSA to notify its employees, however, there must also be a "real risk" of harm to the employee 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.

[16] In deciding whether there exists a "real risk" of harm in this case, I considered that the information at issue was highly sensitive, as it includes website logins and passwords and financial information. I also considered CSA's information that this virus has been linked to organized crime. In my opinion, there is a real risk of harm in this matter.

[17] Given the information reported by CSA, I have decided there is a real risk of significant harm to individuals as a result of this incident. I have based my decision on the following factors: the type of information involved could be used to commit identity theft, which is a significant harm, and the Qakbot virus intentionally targets pre-populated website data, which often includes financial information, passwords and other sensitive personal information.

V. Decision

[18] I understand CSA has already notified all of the affected individuals by way of an email sent on April 5, 2011. I further note that CSA's notification was compliant with s.

19.1 of the PIPA Regulation and therefore I will not require CSA to notify affected individuals again.

Frank Work, Q.C.
Information and Privacy Commissioner