ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-036

GICdirect.com Financial Services Ltd.

November 1, 2011

(Case File #P1991)

I. Introduction

[1] On October 3, 2011, I received a report from GICdirect.com Financial Services Ltd. ("GIC") of an incident involving the loss of 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 GIC 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] 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;

[4] I have jurisdiction in this matter because GIC 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).

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

III. Background

[6] On October 3, 2011, I received a written report from GIC describing an incident involving the loss of personal information.

[7] On October 3, 2011, my Office contacted GIC to request that it provide additional information concerning the incident, in order for me to determine whether to require GIC to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided in a number of telephone calls between October 3, 2011 and October 24, 2011.

[8] The circumstances of the incident as reported to me by GIC are as follows:

- GIC has policies in place which prevent employees from removing client personal information from the office. GIC has additional policies which address the security of personal information under its custody or control including limited access to personal information, technological security measures, confidentiality agreements with employees and employee privacy training.

- Since June 2011, GIC has been upgrading its client management computer system.

- Despite its policies and safeguarding measures, on September 24, 2011, a long-term and valued employee saved client personal information onto a USB memory stick to do some work outside of the office. The data on the memory stick was not encrypted. The employee intended to assist the organization through working from home.

- Unfortunately, sometime between September 24 and 25, 2011, the employee lost the memory stick.

- GIC estimated that up to 489 individuals may have been affected by the loss of the memory stick. Of these 489 individuals, 23 are Albertans. Given the nature of the system upgrade, GIC was unable to determine exactly how many clients had their personal information on the memory stick. GIC erred on the side of caution by identifying a wide range of clients for notification that would include everyone who had been affected and likely some who had not been.

- The personal information contained on the memory stick varied greatly from client to client. Some clients had only their names and addresses on the stick, while other clients may have had names, addresses, social insurance numbers, identification, birthdates and financial information on the memory stick.

- Immediately upon discovery of the loss of the memory stick, the employee notified GIC and conducted a thorough search for the memory stick. The employee also began retracing steps of all locations that were attended during the time period in which the memory stick was lost. The employee left contact information at all locations and offered a reward if the memory stick was located. The employee followed up with all of the locations two days later.

- GIC also notified the police of the loss of the memory stick.

- GIC notified the Office of the Information and Privacy Commissioner for British Columbia on September 28, 2011 of the breach and notified all of its potentially affected clients of the breach on October 3, 2011. In addition to the background circumstances of the breach, GIC included an explanation of the potential risks affected individuals might face and provided detailed information about steps they might take to mitigate the risks. GIC also included information about its privacy practices and the numerous steps it has taken to protect client personal information.

- In light of this incident GIC has reviewed its security measures and has taken steps to improve them where possible. GIC has also provided training to the employee who removed the personal information from the office and has emphasized its policies throughout the organization.

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

[9] Pursuant to section 37.1 of PIPA, I have the power to require GIC 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 GIC to

notify individuals, I must consider whether there exists a "real risk of significant harm" to individuals as a result of the incident.

[10] In order for me to require that GIC notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to those 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.

[11] In this case, the personal information at issue is of high sensitivity as it includes social insurance numbers and individuals' financial details.

[12] GIC 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.

[13] In order for me to require GIC to notify the affected individuals, however, there must also be a "real risk" of significant harm to the employee 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. Further, there must be a cause and effect relationship between the incident and the possible harm.

[14] In deciding whether there exists a "real risk" of harm in this case, I considered that the memory stick was not encrypted and despite numerous attempts to locate it and follow up with the various locations where it may have been found, the memory stick was not recovered. There is a real risk the memory stick could have been found by someone else and that person could use the information for malicious purposes.

[15] Given the information reported by GIC, I have decided that 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 unencrypted memory stick has not been located.

V. Decision

[16] Based on the information reported to me by GIC, I have concluded there is a real risk of significant harm to individuals as a result of this incident and I require GIC to notify affected individuals. I understand GIC has already notified the individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* by way of letters sent on September 28 through October 3, 2011; therefore I will not require GIC to notify again.

Frank Work, Q.C.
Information and Privacy Commissioner