ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-001

AVISCAR INC.

January 6, 2011

(Case File #P1739)

I. Introduction

[1] On December 10, 2010, I received a report from Aviscar Inc. (Aviscar) of an incident involving the loss of and 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 Aviscar notify those individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[2] PIPA applies to to provincially-regulated private sector organizations in Alberta. I have jurisdiction in this case because Aviscar is an "organization", as defined in section 1(1)(i) of the Act, operating in the province of Alberta.

[3] Under section 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.

[4] 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.

[5] In considering whether to require Aviscar 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 December 10, 2010, I received a written report from Aviscar describing an incident involving the loss of and unauthorized access to personal information.

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

- Aviscar contracted with a third party operator (the "TPO") to operate the car rental business located at 10235 101 Street, Edmonton, Alberta (the "Location").
- A report of fraudulent credit card use which was believed to be linked to Aviscar was received from American Express ("Amex") on or about November 8, 2010. Aviscar was further advised of additional reports of fraudulent credit card use from the Royal Bank of Canada ("RBC"). These reports identified 17 credit card numbers (6 from Amex and 11 from RBC) where fraudulent use of the credit card number had been reported over dates ranging from early September to early October, 2010.
- Aviscar worked with Amex, RBC and law enforcement to determine the common source of where the credit cards were used. Aviscar identified the Location as the common source. Law enforcement investigations narrowed the source to of the alleged credit card compromise to the TPO at the Location.
- On November 22, 2010, the TPO was arrested by the Edmonton Police. The TPO was found to have attached a key logger/skimming device, which intercepts information that is input to the computer and stores it on a micro disk, between the swipe device and the computer used to input car rental agreements.
- The Edmonton Police advised Aviscar that the TPO had been charged with a number of crimes including (i) global possession of credit card data to commit fraud, (ii) trafficking in credit card fraud and (iii) possession of a logger/skimming device. The Police further advised Aviscar that the TPO had admitted to using the key logger device from sometime in August or September, 2010. They informed Aviscar that they recovered credit card information on the key logger.
- On December 6, 2010, law enforcement provided confirmation of the transaction information obtained from the recovered key logger device, which included customer's names, credit card numbers and the date of rental.
- The Edmonton Police advised Aviscar that all of the credit card issuers had been notified of the possibility of credit card compromise but that no other incidents of compromise had been reported.
- With respect to the 17 known incidents of fraudulent credit card use, these have been addressed by the card issuers who have issued new credit cards to these account holders.
- Based upon the 17 known instances; the information the TPO provided to the Edmonton Police regarding when he commenced using the key logger; and the information recovered from the key logger device, Aviscar believes the possible time period which the TPO may have obtained credit card information through the key logger to be sometime in August through November 19, 2010.

- Aviscar has identified a maximum of 706 unique credit card transactions at the Location during the time period of August 1, 2010 through November 19, 2010. This total is a compilation of all transactions which used credit cards during that time period. Aviscar has no information whether or not the credit card numbers were captured by the key logger device.
- The individuals affected by this incident are customers who used a credit card to rent a vehicle from the Location between August 1, 2010 and November 19, 2010.
- Aviscar assessed the type of harm that may result from the breach as identity theft and the level of this harm as "Medium".
- Aviscar submitted that this appears to be an isolated incident from the actions of a rogue TPO, although Aviscar considers it to be serious. The credit card fraud identified by Amex and Royal Bank (17 cards) has already been addressed through the issuance of new cards. No other fraudulent credit card use involving this Location or other Aviscar locations in Alberta has been brought to its attention. The Edmonton Police have advised that the credit card issuers were notified and that no additional reports of confirmed credit card compromise have been received. Aviscar is maintaining ongoing communications with law enforcement in the event that additional information becomes available. As the information was stolen, there is a risk of it being used to commit fraud, although this has been mitigated by the arrest of the TPO and the recovery of the key logger device.
- Notification by Aviscar to credit card issuing financial institutions of all cards used at the Location between August 1, 2010 and November 19, 2010 is to be completed by December 22, 2010.
- Aviscar's communication to the issuing banks will mitigate risk to cardholders as the issuing banks will monitor activity on the identified accounts and reissue new cards as required.
- Aviscar has not notified any of the customers whose credit card information may have been compromised and submits if notification is required, it would be most appropriate for the credit card "retailers"[1], as opposed to Aviscar, to advise their customers directly of the appropriation of the credit card information as the "retailers" will be in the best position to determine if the credit card information was subsequently used in a fraudulent manner, or decide whether new cards should be issued. This information will not be available to Aviscar but will be of primary concern to the affected individuals.
- Aviscar is implementing a number of processes and changes to minimize the possibility of such an incident occurring again.

[1] Aviscar does not identify who the credit card "retailers" are it is referring to but I take this to mean either the banks that have issued the credit cards, such as the Royal Bank, or the credit card companies, such as AMEX.

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

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

[9] In order for me to require that Aviscar 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.

[10] In this case, the personal information of the customers is of high sensitivity as it includes customer names and credit card numbers.

[11] As Aviscar noted, this is information that could be used to cause harm to individuals, and provides comprehensive individual profiles that could be used for identity theft and/or fraud. I disagree with Aviscar's assessment that the level of harm is only "Medium". In my view the level of harm of identify theft in this case is "High".

[12] In order for me to require Aviscar 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.

[13] Given the sensitivity of the personal information of the customers at issue, and the fact the information was stolen and has already been used in 17 known cases to commit credit card fraud, I believe there is a real risk of significant harm to the individuals who rented vehicles using their credit cards from the Aviscar Location between August 1, 2010 and November 19, 2010.

V. Decision

[14] Based on the information reported to me by Aviscar, I have concluded there is a real risk of significant harm to the individuals who rented vehicles using their credit cards from the Aviscar Location between August 1, 2010 and November 19, 2010 as a result of this incident.

[15] Aviscar has advised it identified 706 unique credit card transactions at the Location during this time period but does not know whether or not all of these credit card numbers were captured by the key logger device. Accordingly, I require Aviscar to notify **all** individuals who used credit cards to rent vehicles at the Location during this period of the incident in accordance with section 19.1 of the Regulation and confirm in writing to my

Office that it has done so **on or before Monday, February 7, 2011** or such other date as I may specify.

[16] I reject Aviscar's submission that it would be most appropriate for the credit card "retailers", as opposed to Aviscar, to advise the affected individuals of this breach. The incident happened to Aviscar, not the credit card "retailers". PIPA requires the organization having the personal information under its control and which experienced the incident to report the incident and where I determine notification is necessary, to notify the affected individuals. In this case Aviscar is the organization that had the personal information under its control and experienced the incident, not the credit card "retailers". The purpose of notification is to enable individuals to take steps as quickly as possible to avoid or mitigate the possible harm that may arise from the incident. Aviscar's suggestion that it should not be the party to have to notify because it does not know if the customer's credit card has been fraudulently used is not relevant. Whether the customer's credit card has been fraudulently used yet is not the point. The point is to inform the customer of the potential it may be used so the customer can take any steps he or she deems necessary to prevent fraudulent use. Aviscar must notify the affected individuals and provide them with the details of the incident as required by the Regulation.

Frank Work, Q.C.
Information and Privacy Commissioner