ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-010

Twin America LLC

April 18, 2011

(Case File #P1769)

I. Introduction

[1] On February 28, 2011, I received a report from Twin America LLC ("Twin America" or the "Organization") of an incident involving unauthorized access to 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 individuals as a result of the incident, and therefore I require that Twin America 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;

[5] Twin America is a US based corporation with no business presence in Alberta or Canada. Despite this, I have taken jurisdiction because its clients include Albertans and the compromised personal information includes the personal information of Albertans. See: *Lawson v. Accusearch Inc. 2007 FC 125*

[6] Twin America reported that the personal information at issue included names, addresses, email addresses, credit card numbers, credit card expiration dates and CVV2 codes (the 3 digit number on the back of a credit card). The information at issue in this incident qualifies as "personal information" as defined in section 1(1)(k).

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

III. Background

[8] On February 28, 2011, I received a written report from Twin America describing an incident involving the unauthorized access to personal information.

[9] On March 17, 2011, my Office contacted Twin America to request that it provide additional information concerning the incident, in order for me to determine whether to require Twin America to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided in a number of telephone calls on March 17, 2011.

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

- Twin America operates a tour bus company in the United States. It has no business presence in Canada, but some of its customers are Albertans.

- Through its investigation, it determined that Albertans were included amongst the affected individuals, and therefore it reported the breach to this office.

- On or about October 25, 2010, Twin America learned that its customers' credit card information may have been compromised when a web programmer discovered unauthorized script that appears to have been uploaded to the Organization's web server.

- The unauthorized script was a SQL injection script which appeared to have occurred on September 26, 2010. It successfully permitted hackers unauthorized

access to the Twin America database from September 26, 2010 to October 19, 2010.

- The personal information accessed in the database included:
    - Cardholder name;
    - Address;
    - Email address;
    - Credit card number;
    - Expiration date; and
    - CVV2 (the three digit code on the back of a credit card).

- Upon discovery of the incident, Twin America took numerous appropriate actions to respond to the breach including:
    - Investigating the situation to determine what had happened and what information had been accessed;
    - Filing a complaint with the FBI Internet Crime Complaint Centre;
    - Filing a police report with the New York City police;
    - Retaining legal counsel to oversee forensics and coordinate an appropriate data breach response;
    - Retaining a privacy breach company to investigate the incident and assist Twin America with its response;
    - Notification to credit card processors and credit card brands; and
    - Preparation of notices to affected individuals and applicable regulatory authorities, such as the Alberta Privacy Commissioner to explain the incident and outline the steps taken to contain and manage the incident.

- Twin America determined that of the individuals affected by the breach, approximately 670 of them were Albertans; that is, the addresses they had provided the Organization identified them as living in Alberta.

- Twin America confirmed it had already notified affected individuals, including Albertans, via email and provided a copy of its notification. The notification advised affected individuals to remain vigilant by reviewing account statements and offered call centre support.

- As a result of the incident, Twin America has taken numerous steps to prevent a reoccurrence including:
    - Increasing the profile of data security incidents throughout the Organization;
    - Changing all administrative passwords and enforcing stronger complexity rules;
    - Restricting access to the “admin panel” and server;
    - Identifying and remediating database scripting vulnerabilities and installing an application firewall to prevent further attacks;
    - Conducting independent penetration tests;

- Reconfiguring its systems such that transactions can be processed without storing credit card information on the Organization's servers; and
- Twin America continues to work with the privacy breach company and other consultants to further enhance network security, company policies and procedures and other protections.

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 Twin America 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 Twin America 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 Twin America 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.

[13] In this case, the personal information at issue is of high sensitivity as it includes cardholder names and addresses in addition to credit card numbers, expiration dates and CVV2 numbers.

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

[15] In order for me to require Twin America to notify affected Albertans, however, there must also be a "real risk" of harm to the 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.

[16] In deciding whether there exists a "real risk" of harm in this case, I considered the unauthorized script had been used to access the credit card information in the database. It is obvious, given the nature of the unauthorized script and the information that the individuals who accessed it did so for nefarious purposes.

[17] Given the information reported by Twin America, 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 fraud and identity theft, which is a significant harm.

V. Decision

[18] Based on the information reported to me by Twin America, I have concluded there is a real risk of significant harm to individuals as a result of this incident and I require Twin America to notify affected individuals in Alberta. I understand Twin America has already notified affected individuals via email in accordance with section 19.1 of the *Personal Information Protection Act Regulation*, and therefore, I will not require Twin America to notify again.

Frank Work, Q.C.
Information and Privacy Commissioner