ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-042

PERSONALITY PROFILE SOLUTIONS INC.

November 1, 2011

(Case File #P2003)

I. Introduction

[1] On October 14, 2011, I received a report from Personality Profile Solutions Inc. ("PPSI" or the "Organization") 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 PPSI 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] I have jurisdiction in this matter because PPSI 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).

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

III. Background

[7] On October 14, 2011, I received a written report from PPSI describing an incident involving the unauthorized access to personal information.

[8] On October 24, 2011, my Office contacted PPSI to request that it provide additional information concerning the incident, in order for me to determine whether to require PPSI to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided in a telephone call and e-mail correspondence between October 24, 2011 and October 26, 2011.

[9] The circumstances of the incident as reported to me by the Organization are as follows:

- On September 14, 2011, PPSI discovered that unknown person(s) illegally accessed the system of the outside vendor that hosts their website: DISCProfile.com. It was found that credit card transactions processed between May 8, 2011 and September 14, 2011 were subject to illegal interception.
- In early September, 2011 (prior to September 14) three customers outside of Canada notified PPSI about fraudulent credit card transactions. After receiving these customer notifications, PPSI immediately engaged their website development firm to review the shopping cart on the DISCProfile.com website for fraudulent credit card transactions. On September 14, 2011, this website development firm notified PPSI and its outside vendor website host that this hack had occurred.

- There were a total of 2 affected Albertans that had purchased products online using the DISCProfile.com website between May 8, 2011 and September 14, 2011. The customer personal information at issue included:
    - Name;
    - Address;
    - Telephone number;
    - Credit card number;
    - Credit card expiration date; and,
    - Credit card CVV number.
- PPSI notified the FBI who conducted an investigation into the incident. At the time this breach report was submitted to this Office, the FBI investigation was still ongoing. The Organization already used encryption on its website, but as a result of the incident, PPSI has improved its encryption and detection safeguards on its website.
- PPSI notified the affected individuals on October 25, 2011, and has provided the affected individuals with one year of free credit monitoring.

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

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

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

[12] In this case, the personal information at issue is of high sensitivity as it includes customer name and current credit card information. The Organization stated that some customers (not those affected in Alberta), had experienced credit card fraud when they discovered fraudulent charges to their cards. It was though the notification to PPSI by those customers that the investigation into the hack was started. I believe that personal information at issue in this case is of high sensitivity, and is (and clearly was as it was used fraudulently) of value to those who commit theft. The type of harm that could result from the unauthorized access to this personal information is identity theft, which, in my view, is a significant harm.

[13] In order for me to require PPSI to notify its affected customers, however, there must also be a "real risk" of significant harm to the customers 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 significant harm in this case, I considered that the personal information is sensitive in nature and could be used to commit identity theft. The information was obtained via a hack, which is a clear indication of theft by individual(s) with nefarious intentions.

[15] Given the information reported by PPSI, 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; credit card transactions were illegally intercepted over a period of more than four months prior to being detected; and, the incident is the result of a hack by individual(s) with malicious intent who subsequently used credit cards fraudulently.

V. Decision

[16] Based on the information reported to me by PPSI, I have concluded there is a real risk of significant harm to individuals as a result of this incident, and I require PPSI to notify the affected individuals. I understand PPSI has already notified the individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* by way of letter sent on October 25, 2011; therefore I will not require PPSI to notify again.

Frank Work, Q.C.
Information and Privacy Commissioner