ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2013-ND-22

Dealertrack Canada, Inc.

October 24, 2013

(Case File # P2314)

I. Introduction

[1] 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.

[2] On April 22, 2013, **Dealertrack Canada, Inc.** ("the Organization") provided notice of an incident of unauthorized access to personal information. For the reasons that follow, I have decided that there is a real risk of significant harm to individuals as a result of the incident. I require that the Organization notify the individuals to whom there is a real risk of significant harm.

II. Jurisdiction

[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] The Organization is headquartered in Mississauga, Ontario and is registered in Alberta as an extra-provincial corporation. Therefore, I have jurisdiction in this matter because the Organization is an "organization" as defined in section 1(1)(i) of PIPA.

[6] The Organization reported the incident involved the following information, collected from eight individuals residing in Alberta:

- name,
- address,
- phone number (home and mobile),
- last three digits of Social Insurance Number,
- date of birth,
- gender,
- marital status,
- email address,
- duration of residence at current address,
- previous address,
- home ownership status,
- mortgage details, including payment amount,
- current employment information, including employer, length of service, and employment status, and
- income details.

[7] This information qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

III. Background

[8] On May 12, 2013, my Office requested the Organization provide additional information. The additional information was provided by the Organization May 13, 2013.

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

- The Organization operates a computer system used by auto dealers to communicate electronically with potential lenders and insurers.
- On April 5, 2013, a fraudulent caller claiming to represent the Organization's technical support contacted two employees of an auto dealer and convinced them to provide their login credentials.
- Using these credentials, an intruder logged into the Organization's system and attempted to access credit bureau reports for auto dealer customers.
- The attacker was able to view and print the personal information noted above for eight individuals.
- Information security measures prevented access to credit bureau reports and allowed the Organization to detect and terminate the intruder's access.
- System logs show the intrusion was limited to April 5, 2013, from 9:10 pm to 10:56pm (Eastern Time), when the Organization terminated the access.
- The Organization confirmed the auto dealer sent a letter about the incident to the eight affected individuals via registered mail on April 16, 2013.

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

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

[11] Pursuant to section 37.1 of PIPA, I have the power to 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." In determining whether or not to require the Organization to notify the affected individuals, I must consider if there is a "real risk of significant harm" to the affected individuals as a result of the incident.

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

[13] The Organization believes the information could be used for the purpose of identity theft or other fraudulent activity.

[14] While the intruder did not gain access to credit bureau information, the personal information that was accessed is of high sensitivity. It includes the affected individuals' birth dates, financial information and employment history. The type of harm that could result from unauthorized access to the personal information in this instance is identity theft or fraud. In my view, these are significant harms.

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

[16] P2012-ND-02 involved a similar incident with the same Organization, in which the same highly sensitive personal information was accessed. In this case, it was decided there was a real risk of significant harm to the individuals affected.

[17] Based on the above and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individuals as a result of this incident. In making this decision, I considered that the personal information at issue is of high sensitivity and that the intruder's intent was malicious. The intruder demonstrated malicious intent by impersonating the Organization's technical support to mislead the auto dealership's employees into revealing their login credentials. Further, system logs indicate the intruder viewed and printed the affected individuals' personal information. In my view, these factors, together with the nature of the personal information involved, indicate there is a real risk of significant harm to the affected individuals as a result of this incident.

V. Decision

[18] I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (the "Regulation").

[19] I understand that the Organization has notified the affected individuals through the auto dealer in accordance with the Regulation in a letter sent on April 16, 2013. Therefore, I will not require the Organization to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner