ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-02

DealerTrack Canada, Inc.

February 22, 2012

(Case File #P2037)

I. Introduction

[1] On November 17, 2011, I received a report from DealerTrack Canada, Inc. ("DealerTrack" 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 the affected individual as a result of the incident, and therefore I require that DealerTrack notify the individual 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 DealerTrack is an "organization" as defined in section 1(1)(i) of PIPA and has control of the information, 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 DealerTrack 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 November 17, 2011, I received a written report from DealerTrack describing an incident involving the unauthorized access to personal information. The incident was the result of a malicious attack in an attempt to gain access to credit bureau reports.

[8] On November 22, 2011, my Office contacted DealerTrack to request that it provide additional information concerning the incident, in order for me to determine whether to require DealerTrack to notify the individual under subsection 37.1(1) of PIPA. The additional information was provided in a number of e-mails and telephone calls between November 22, 2011 and February 6, 2012.

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

- In violation of its agreement with DealerTrack, a user of the DealerTrack Canada internet site at an automotive dealership (located in Edmonton, Alberta) provided answers to their password recovery information. This allowed an individual posing as a DealerTrack employee to fraudulently gain access and reset the dealership user's DealerTrack login password. Subsequently, the credentials were then used to view one consumer file on the DealerTrack internet site. The incident occurred on September 11, 2011, and was discovered on the same day

when an automated system check alerted DealerTrack to an abnormal pattern of activity.

- DealerTrack acts as a conduit between the dealership and lending institutions. The dealership designated administrative users are granted access and are responsible for granting and revoking access to other dealership employees. The dealership employees collect the consumer's information after gaining informed consent.
- DealerTrack subsequently submits the information to the lending institutions for the purpose of approving or declining a loan or lease for vehicle purchase.
- The personal information at issue for the one affected individual in this case is:

    - Name;
    - Address;
    - Phone number (home and mobile);
    - Social insurance number (masked except last three digits viewable);
    - Date of birth;
    - Gender;
    - Marital status;
    - E-mail address;
    - Duration of residence;
    - Previous address;
    - Home ownership status;
    - Mortgage payment amount;
    - Current employment information including employer, length of service, and employment status; and,
    - Income details.

- DealerTrack was able to confirm that the above is the personal information accessed as it had a detailed audit logging report of actions performed in the system.
- DealerTrack believes that the attacker's primary intention was to gain access to DealerTrack's ability to access consumer credit reports. A technical control put in place prior to a dealership being granted credit bureau access prevented this from occurring (the viewing of consumer credit reports). As the perpetrator could not gain access to credit reports as a result of this technological control, s/he clicked through the affected individual's consumer file in an attempt to access the credit bureau functionality from a different access point. While this access was also blocked, during the attempt, the consumer's personal information was viewable by the attacker.
- DealerTrack has not been able to identify the perpetrator, and has involved the RCMP who are conducting an investigation into the matter.
- The affected individual was notified of the incident on October 27, 2011 by the dealership in question.

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 DealerTrack 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 DealerTrack to notify the affected individual, 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 DealerTrack notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to the consumer 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 name, address, date of birth, last three digits of social insurance number, home ownership status and payment amounts, and employment information of the affected individual.

[13] DealerTrack 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. In addition, DealerTrack confirmed that it believed the access to be intentional and malicious in an attempt to gain access to personal information.

[14] In order for me to require DealerTrack to notify the affected individual, however, there must also be a "real risk" of significant harm to the individual 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.

[15] In deciding whether there exists a "real risk" of significant harm in this case, I considered that the personal information at issue is of high sensitivity and that the attack was malicious in its intent to gain access to the affected individual's personal information. While the perpetrator was not able to gain access to the credit bureau functionality, the perpetrator demonstrated his/her malicious intent to do so by impersonating a DealerTrack employee and contacting an individual at the dealership and successfully gaining access to their username and password. In my view, the type of personal information accessed by the perpetrator, combined with the actions of that individual suggests that there is a real risk of significant harm to the affected individual.

V. Decision

[16] Based on the information reported to me by DealerTrack, I have concluded that there is a real risk of significant harm to the affected individual as a result of this incident. DealerTrack has provided notification to the affected individual; however, that

notification did not contain all of the requirements pursuant to section 19.1 of the *Personal Information Protection Act Regulation*.

[17] I order that re-notification is required on section 19.1(1) (b) (ii) and (iv). DealerTrack will need to provide the affected individual with the date the incident occurred as well as additional information on the steps the Organization has taken to reduce the risk of harm. DealerTrack is required to confirm it has done so in writing to this Office, on or before March 14, 2012.

Jill Clayton
Information and Privacy Commissioner