ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-007

Agritrac Equipment Ltd.

April 12, 2011

(Case File #P1820)

I. Introduction

[1] On April 1, 2011, I received a report from Agritrac Equipment Ltd. ("Agritrac" or the "Organization") 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 Agritrac 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 Agritrac 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). There is no evidence before me that Agritrac is providing services to any of the other involved organizations under s. 5(2). Therefore, if notification is required, it is Agritrac's responsibility to do so.

[6] In considering whether to require Agritrac 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 April 1, 2011, I received a written report from Agritrac describing an incident involving the loss of and unauthorized access to personal information.

[8] Prior to receiving the report, my office had been in communications since late February 2011 with Agritrac and three other organizations regarding the circumstances of this breach. Two of the other involved organizations also provided me with breach reports. The information required for me to determine whether there is a real risk of significant harm, and which organization(s) have an obligation to notify affected individuals was provided to me by the involved organizations from approximately February 28, 2011 to April 1, 2011 through a series of written communications, emails and telephone calls.

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

- Agritrac is an active Alberta corporation and a farm equipment rental company.

- In approximately December 2010/January 2011, various assets of Agritrac were split into two new organizations, one of which also submitted a breach report to this office. Agritrac remained an active corporation on the Alberta corporate registry.

- Prior to the above noted transaction, in order to obtain farm equipment, many of Agritrac's customers applied for financing from a financing company (the "Financing Company").

- In order to obtain financing, Agritrac customers would provide information on the Financing Company's application form. Agritrac would then transfer the information on the application form electronically to the Financing Company for

review and Agritrac would keep the physical paper copies of the application form in a locked storage room.

- Information on the Financing Company's application forms included, but was not limited to:
    - Name;
    - Date of birth;
    - Social insurance number;
    - Address and contact information;
    - Occupation information;
    - Annual gross income and net worth;
    - Bank account number (and bank contact information); and
    - Approximate chequing account balance.

- In approximately July 2010, there was a break-in at Agritrac's office. The break-in was reported to police and investigated, but at the time, Agritrac believed that none of its records had been stolen. After the involved organizations were notified of this incident, Agritrac conducted another review and determined that a bankers box of financing application forms had disappeared. Agritrac believed that the bankers box of forms was likely stolen during the July 2010 break-in.

- On January 26, 2011, the Financing Company was contacted by the Edmonton Police Service ("EPS"). During a raid, the EPS had discovered credit applications for 70 individuals on the Financing Company's application forms.

- The Financing Company conducted an internal investigation and determined that the application forms appeared to have originated from Agritrac. The Financing Company, Agritrac, EPS and the two other organizations that had purchased Agritrac's assets were all in communication with each other at various times regarding the breach.

- EPS indicated that at least one of the 70 affected individuals had been a victim of identity theft. As its investigation was still ongoing, EPS had not shared all of its information with Agritrac or the other involved organizations, but it did provide the names of 63 of the 70 individuals affected by the breach.

- EPS also stated it notified some of the affected individuals about the breach.

- All of the organizations that reported this breach to the OIPC are of the opinion that the most likely explanation for the breach is that a bankers box of financing application forms was stolen from Agritrac during the July 2010 break-in.

- In its report to me, Agritrac stated it planned to notify affected individuals of the breach by April 6, 2011.

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

[10] The circumstances of this breach are somewhat unusual in that three separate organizations reported it to my office. Pursuant to section 37.1 of PIPA, I have the power to require an 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." All of the organizations agree that the application forms recovered by EPS likely originated from Agritrac's office during the July 2010 break-in. One of the organizations that reported the breach to this office had no relation to Agritrac at the time of the break-in, but purchased many of Agritrac's assets in December2010/January 2011 and has indicated its willingness to notify affected individuals if ordered to do so, or to assist another organization with notification. The Financing Company did not ever have custody or control of the physical application forms because the information it collected on the forms was transferred to it electronically by Agritrac; however it has also indicated its willingness to notify, or to assist another organization with notification.

[11] Agritrac remains an active corporation on the Alberta corporate registry and has indicated its intention to notify the affected individuals. Given the particular facts before me including the widely-held assumption that the application forms were within Agritrac's custody and control at the time of breach and Agritrac's stated intention of notifying affected individuals, I find that the responsibility for notification rests primarily with Agritrac, not with the other organizations that reported the breach to me.

[12] In determining whether or not to require Agritrac to notify individuals, I must consider whether there exists a "real risk of significant harm" to individuals as a result of the incident.

[13] In order for me to require that Agritrac notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to the affected 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.

[14] In this case, the personal information at issue is of high sensitivity because it includes detailed financial information.

[15] Agritrac also noted that the type of harm that could (and has) resulted from the unauthorized access to or disclosure of this information is identity theft, which, in my view, is a significant harm.

[16] In order for me to require Agritrac to notify affected individuals, however, there must also be a "real risk" of harm to the employee 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.

[17] In deciding whether there exists a "real risk" of harm in this case, I considered the fact that EPS confirmed at least one case of identity theft has already occurred as a result of this breach and the sensitivity and detail of the financial information makes it likely that more cases of identity theft could (or may already have) occurred.

[18] Given the information reported by Agritrac, 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 and has been used to commit identity theft, which is a significant harm.

V. Decision

[19] Based on the information reported to me by Agritrac, I have concluded there is a real risk of significant harm to individuals as a result of this incident and I require Agritrac to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation*, and confirm in writing to my Office that it has done so on or before May 3, 2011 or such other date as I may specify.

Frank Work, Q.C.
Information and Privacy Commissioner