ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-033

ASSANTE WEALTH MANAGEMENT

December 14, 2011

(Case File #P1959)

I. Introduction

[1] On August 15, 2011, I received a report from Assante Wealth Management ("Assante" 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 Assante 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 Assante 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 Assante 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 August 15, 2011, I received a written report from Assante describing an incident involving the loss of and unauthorized access to personal information. The privacy breaches identified by Hein Financial Group ("Hein") and Assante appear to have impacted clients at a number of financial institutions, including:

- CI Investments Inc. ("CI");
- Sun Life Financial ("Sun Life"); and,
- Manulife Bank of Canada ("Manulife").

[8] On August 29, 2011, my Office contacted Assante to request that it provide additional information concerning the incident in order for me to determine whether to require Assante to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided in a telephone call.

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

- On May 19, 2011, CI Investments' Toronto, Ontario based operations was alerted to suspicious account activity in regards to client accounts serviced by the Hein Financial Group. Hein Financial Group provides financial advice to clients in Alberta and Saskatchewan.
- Upon notification of the suspicious activity, Assante's compliance department began an investigation.

- *Assante/CI Investments:*
    - Assante and CI concluded that some Hein clients had their personal information accessed on an unauthorized basis between March 14, 2011 and June 8, 2011. It is believed that the unauthorized party gained access to the clients' personal information at CI by using the password of an employee of Hein to access an online CI database. The unauthorized party made use of the clients' personal information to contact CI in an attempt

to obtain additional personal information of those clients and subsequently redeem and misappropriate assets held in CI accounts serviced by Hein.
    - The personal information at issue that may have been accessed includes, but is not limited to: client names, addresses, SIN, and other financial information including account numbers, holdings, and transaction activity at CI.
    - It is confirmed that 10 CI clients had their personal information accessed on an unauthorized basis. It is confirmed that the unauthorized party successfully redeemed and misappropriated funds from two client accounts at CI and attempted to withdraw funds from a third.
    - It is believed that an additional 32 CI clients' personal information may have been accessed on an unauthorized basis.
    - In total, all 42 clients have been notified of the incident.

- *Assante/Sun Life:*
    - On July 7, 2011, Hein became aware of suspicious activity with respect to a client's universal life policy at Sun Life.
    - Assante and Sun Life have identified four Sun Life clients who have had their personal information accessed on an unauthorized basis. The unauthorized party attempted to redeem and misappropriate funds through an electronic funds transfer from one client's universal life policy. The funds transfer was successfully executed; however, the bank had frozen the account due to suspicious activity and the transfer was stopped.

- *Assante/Manulife:*
    - On July 12, 2011, Manulife Bank was notified by Hein of a privacy breach at the branch. A preliminary assessment was conducted to identify the impacted clients and develop a mitigation strategy to protect client accounts. Manulife identified 154 bank accounts belonging to the clients of Hein, and each of these 154 accounts was flagged for enhanced authentication.
    - On July 18, 2011, Manulife was notified of suspicious activity within one Manulife bank account which occurred on July 11, 2011. An investigation revealed that one bank account was accessed on an unauthorized basis where a sum of money was transferred to a bank account at another financial institution.
    - A further three bank accounts showed activity that indicated attempted, but unsuccessful, unauthorized access.

- Assante reported the steps it took following the breach to reduce the risk of harm to individuals. Some of these steps include:
    - Restricting client accounts;
    - Notifying fund companies and financial institutions that Hein deals with on behalf of its clients;

    - Review of security files and controls, review of third party contractor relationships and access to the branch, sub-branch access and controls to client information and advisor passwords;
    - Communicating requirements of staff passwords and controls and access.
- Assante has reported that it sent notifications to all of its Advisor's clients in addition to the individuals known to have been affected.
- It is still unknown who accessed the personal information of those affected.

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 Assante 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 Assante 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 Assante notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to Assante's clients 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 client's name and address, social insurance number, and financial information.

[13] In its assessment of harm resulting from the breach, Assante believes there is a high risk that harm could result for those clients whom they confirmed had their accounts accessed. This harm was noted as identify theft.

[14] In order for me to require Assante to notify its clients, however, there must also be a "real risk" of significant harm to the clients 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 includes full name and address, social insurance number, and financial information of individuals. This is information that could be used to commit identity theft, which in my view is a significant harm. In addition, it is known that the information was accessed illegally and by an individual(s) with nefarious intentions. The individual(s) who had unauthorized access to client personal information subsequently used that information for monetary gain and made attempts, and was successful in some cases, at misappropriating funds of Hein clients.

[16] Given the information reported by Assante, 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 was) used to commit identity theft, which in my view is a significant harm, and the information was accessed by an external hacker and used with nefarious intentions and for monetary gain.

V. Decision

[17] Based on the information reported to me by Assante, I have concluded there is a real risk of significant harm to individuals as a result of this incident. I acknowledge that Assante has already notified the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation*. As such, I do not require Assante to notify again.

Marilyn Mun
Assistant Commissioner