ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-025

DWM Securities Inc.

August 5, 2011

(Case File #P1931)

I. Introduction

[1] On July 18, 2011, I received a report from DWM Securities Inc., ("DWM" 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 DWM 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 DWM 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] DWM is a regulated, legal entity under the brand name DundeeWealth. DWM has registered advisors (independent franchisees) who are agents of DWM, but not employees. There is a Representative Agreement between DWM and the Advisor. In this determination about which organization was responsible for reporting the breach to this Office, I note that section 34.1(1) of PIPA states that "an organization having personal information under its *control* must… provide notice…" [emphasis added]. It was determined that DWM has control of the client personal information at issue. While the Advisors collect and manage client personal information, DWM is the owner of the data, and DWM has authority over that data as is relates to legal requirements to maintain that data.

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

III. Background

[8] On July 18, 2011, I received a written report from DWM describing an incident involving the loss of, and unauthorized access to personal information.

[9] On July 25, 2011, my Office contacted DWM to discuss details regarding the incident, and obtain further clarification on some points in order for me to determine whether to require DWM to notify individuals under subsection 37.1(1) of PIPA. The unauthorized access to personal information of DWM clients occurred on June 15, 2011.

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

- On June 15, 2011, in Langley, British Columbia, a car belonging to the administrative assistant of two DWM Advisors was broken into, and items in the car were stolen, including an external hard drive. The external hard drive contained an unencrypted backup of the Advisors' internal network, including client files.
- DWM states that it appears this was a crime of opportunity. The external hard drive was contained in a gym bag in the car of the administrative assistant.
- As part of the contract between DWM and its Advisors, the Advisors are required to take reasonable precautions to safeguard client information against loss or

unauthorized access. As part of the Advisors' compliance with the contract between them and DWM, the Advisors were in the process of creating back-ups of their network for the purposes of business continuity planning (BCP) and disaster recovery planning (DRP).

- A requirement of BCP and DRP is that back-ups of the network be stored in an offsite location. For these Advisors, that location was the home of the administrative assistant (who had her car broken into). The administrative assistant stopped on her way home from work on the day she was transferring the hard drive to her home when her car was broken into.
- The client personal information at issue as a result of the breach included copies of client account opening forms which contained the following:

    - First, middle, and last name;
    - Home address;
    - SIN;
    - Date of Birth;
    - Income;
    - Place of Employment;
    - Banking information; and,
    - Copies of relevant identification documents and other government issued identification

- The total number of individuals affected in Alberta were two (2). There were 521 other affected individuals residing in Ontario, California, Michigan, Washington State, and most live in British Columbia.
- DWM is in the process of notifying affected individuals of the breach via telephone. Clients of DWM will be offered a one year subscription to a credit monitoring service at the expense of the Organization.
- Measures taken by DWM following the breach include a review of its policies and procedures regarding privacy and the protection of personal information. Planned changes include the following:
    - Revising its Advisor agreements to specify specific network security standards and require encryption of all information transferred to portable media;
    - Updating the privacy e-Learning course provided to advisors to include additional materials on information security practices.

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

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

[12] In order for me to require that DWM notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to those 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. Numerous factors are considered when determining whether a real risk of significant harm has occurred, which include but are in no way limited to: the magnitude of the breach, that is the number of affected individuals, the maliciousness of the breach including whether there are indications personal information was misappropriated for nefarious purposes, the sensitivity of the information and the harm that may result. Each breach must be assessed based on the circumstances of that particular case.

[12] In this case, the personal information at issue is of high sensitivity as it includes, among other data elements, name, address, SIN, date of birth, banking information, and copies of government issued identification of the individuals. This information is information that could be used to cause significant harm to individuals; most notably, this is information that could be used for identity theft. In effect, criminals could easily build a profile with only a few of these data elements.

[13] In order for me to require DWM to notify its clients, however, there must also be a "real risk" of significant harm to the 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. 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 information at issue is of high sensitivity; that the personal information on the hard drive was unencrypted and going to the home of an administrative assistant; and, that even though the theft of the hard drive was not a targeted theft (other cars were vandalized in the same parking lot at the same time), it was a theft nonetheless.

[15] Given the information reported by DWM, I have decided that there is a real risk of significant harm to individuals as a result of this incident.

V. Decision

[16] I require DWM to notify affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation*, if DWM has not already done so, and confirm to my Office in writing that it has done so on or before August 16, 2011, or such other date as I may specify.

Frank Work, Q.C.
Information and Privacy Commissioner