ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2010-ND-003

TD INVESTMENT SERVICES INC.

August 26, 2010

(Case File #P1644)

I. Introduction

[1] On July 22, 2010, I received a report from TD Bank Financial Group (TDBFG) of an incident involving TD Investment Services Inc. (TDIS) and the unauthorized access to and disclosure of personal information. Based on the information reported to me, I have decided that there is a real risk of significant harm to an individual as a result of the incident, and therefore I require that TDIS notify the individual to whom there is a 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 signification 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] TDBFG reported that the information at issue in this incident consists of a customer's "[n]ame, address, SIN, RRSP account number, and … client number [with another financial institution] …".

[5] This is information about an identifiable individual and so qualifies as "personal information" as defined in section 1(1)(k) of PIPA.

[6] TDBFG also reported that TDIS "is provincially incorporated in Ontario, [and] files in all provinces to be able to carry on business in all those provinces, and is a distinct entity [from TDBFG]."

[7] 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;

[8] I have jurisdiction in this matter because TDIS is a provincially-regulated entity, operating in the province of Alberta, and qualifies as an "organization" pursuant to section 1(1)(i) of PIPA. The personal information at issue is that of a TDIS customer who is a resident of Alberta.

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

III. Background

[10] On July 22, 2010, I received a written report from TDBFG describing an incident involving TDIS and the unauthorized access to and disclosure of personal information.

[11] On August 11, 2010, my Office contacted TDBFG to request additional information regarding this incident. Additional information was provided in telephone calls and through email correspondence between August 11-20, 2010.

[12] In summary, the circumstances of the incident reported to me are as follows:

> *A resident of Alberta who is a [TDIS] customer wished to transfer their [TDIS] mutual fund RRSP account to an account with another financial institution. As part of this request, the customer completed the appropriate form and faxed it to the other financial institution (OFI) on June 10th, 2010. The OFI then faxed the form to [TDIS]'s RRSP transfer processing department on June 22nd, 2010. Upon review by the [TDIS] RRSP transfer processing department, some data on the*

> *form was unclear which required that the form be faxed back to the OFI on June 22nd, 2010.*
>
> *Unfortunately, the [TDIS] employee processing the transfer inadvertently sent the fax to the number from which the customer's initial fax to the OFI originated rather than to the OFI's fax number. This error caused the form to be sent to the customer's workplace without their knowledge.*
> …
>
> *The customer was notified by a coworker that their documentation was on the fax machine.*
> …
>
> *When the customer became aware of this incident they notified TDBFG on June 23rd , 2010.*

[13] Following this incident, TDBFG reported that it "… offered the customer a complimentary subscription to a credit bureau monitoring service in order to reduce their risk of identity theft" and further, that …

> *… to avoid such occurrences in the future, the manager of the TDBFG employee that accidentally faxed the information has discussed this situation with the employee as an opportunity for improvement. Furthermore, a communication regarding the importance of accurate processing will be issued to other employees within the Business Unit.*

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

[14] Pursuant to section 37.1 of PIPA, I have the power to require TDIS 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 TDIS to notify the individual in this case, I must consider whether there exists a "real risk of significant harm" to that individual as a result of the incident.

[15] In order for me to require that TDIS notify the individual, there must be some harm – some damage or detriment or injury – that could be caused as a result of the incident; moreover, that harm must be "significant" – it must be important, meaningful, and with non-trivial consequences or effects.

[16] In this case, the personal information at issue is of moderate to high sensitivity as it includes the individual's "[n]ame, address, SIN, RRSP account number, and … client number [with another financial institution] …".

[17] In its report to my Office, TDBFG reported that:

> *The customer's personal information was faxed to an incorrect number and was not safeguarded. The number was the fax machine in the customer's workplace; therefore, the possibility exists an individual with access to their workplace's fax machine may have recorded the customer's personal information.*

[18] TDBFG also 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.

[19] In order for me to require TDIS to notify individuals, however, there must also be a "real risk" of harm to the individual as a result of this 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.

[20] In deciding whether there exists a "real risk" of harm in this case, I considered that TDBFG reported:

> *The fax was sent by TDIS on June 23, 2010 at 10:23 a.m. The client confirmed that the fax was placed on her desk later that day when she returned from a meeting; however, she was unable to provide a time when the document was collected from the fax machine or deposited on her desk.*

[21] TDBFG also reported that "[t]he client indicated to TDIS that the fax machine is accessible to other employees, but could not provide a precise number."

[22] Given the information reported by TDBFG, I have decided that there is a real risk of significant harm to the individual as a result of this incident. I have based my decision on the following factors: the type of information involved could be used to commit identity theft, which is a significant harm; TDBFG was not able to confirm how long the errant fax was left on the recipient fax machine, nor the number of individuals that might have had access to it. I might have been convinced that there was no real risk of significant harm if the information was exposed for only a short period of time, or if the number of individuals possibly having access to it was relatively small. However, because TDBFG was unable to confirm these details of the incident, I cannot ignore the possibility that the information was exposed to a large number of people for a relatively lengthy period of time.

V. Decision

[23] Based on the information reported to me by TDBFG, I have concluded there is a real risk of significant harm to the individual as a result of this incident. I acknowledge that the individual is aware of this incident as she brought it to the attention of TDIS; however, section 37.1(1)(a) of PIPA gives me the power to require that TDIS notify the individual "in a form and manner prescribed by the regulations." Therefore, I require TDIS to notify the individual of this incident in accordance with section 19.1 of the *Personal Information Protection Act Regulation*, if it has not already done so.

Frank Work, Q.C.
Information and Privacy Commissioner