ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2012-ND-03

J. Darcy Walls Professional Corporation

February 22, 2012

(Case File #P2059)

I. Introduction

[1] On February 6, 2012, I received a report from J. Darcy Walls Professional Corporation ("JD Walls" 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 individuals as a result of the incident, and therefore I require that JD Walls 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 JD Walls 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 JD Walls 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 February 6, 2012, I received a written report from JD Walls describing an incident involving the unauthorized access to personal information.

[8] On February 7, 2012, my Office contacted JD Walls to request that it provide additional information concerning the incident, in order for me to determine whether to require JD Walls to notify individuals under subsection 37.1(1) of PIPA. The additional information was provided in a number of telephone calls and e-mail correspondence between February 8, 2012 and February 13, 2012.

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

- On February 6, 2012, the President of JD Walls reported that his rental unit was burglarized in Cathedral City, California. The thief stole an assortment of goods, including an Ipod and Ipod player, two briefcases, jewellery, spare keys to the President's minivan and rental unit, a camera case and telephoto lens.

- Among the goods stolen from the rental unit was the President's laptop, and hard disk backup that he used to provide his clients with accounting, income tax preparation and financial statement preparation services. It was determined that

the stolen laptop, and hard drive backup contained personal information of 600 former and current clients of the Organization.

- Of the total individuals 560 Alberta residents were affected.

- The personal information stored on the laptop and hard disk backup include:

    - First and last name
    - Home address
    - Email addresses of 20 clients
    - Date of birth
    - Telephone numbers
    - Social insurance number
    - Spouse's name
    - Dependent's name(s)

  There was also 2800 personal income tax returns stored on the hard drive of the laptop containing personal information.[1]

- On the laptop there was no encryption or password protection of the electronic files that maintained the personal information of the affected individuals.

- At the time the incident occurred, the rental unit located in a gated security protected community was securely locked. The security personnel monitor the security gate and patrol the gated community 24 hours a day, 7 days a week.

- Access is limited to residents who have a current transponder (expires at set times) and service providers require written authorization to enter the premises.

- There was an alarm system in the rental unit; however it was not available as it was not completely installed nor activated by the landlord.

- The President of JD Walls immediately reported the incident to the security personnel of the gated community, and Cathedral City Police Department. He advised that the police are continuing with its investigation of the matter. The stolen laptop and hard disk backup along with the other stolen goods have not been recovered.

- The President also reported the incident to the Chartered Accountants of Alberta who referred him to this Office. Additionally, the Organization plans to submit its

[1] The Canada Revenue Agency's Personal Income Tax form includes personal contact information, information about your residence, marital status, information about your spouse or common-law partner and dependents, net income, kinds of income, investments, pension amounts, child care expenses, moving expenses, eligible tuition fees, and other areas. In this case, 2800 personal income tax returns (electronic records) were stolen which involved 450 former clients and 150 current clients.

breach report to the Office of the Privacy Commissioner of Canada and the Office of the Information and Privacy Commissioner of British Columbia.

- JD Walls notified 20 affected Alberta clients by telephone shortly after the incident. The Organization is in the process of notifying affected individuals of the breach by written notification and by telephone.

- The Organization noted that clients of JD Walls will be offered credit monitoring service at TransUnion and Equifax.

- The Organization outlined its long term strategies regarding privacy and protection of its clients' personal information. These strategies are:

    - Change the Canada Revenue Agency password to file 2011 tax returns;
    - Assess the implementation of cloud computing services for offsite storage and daily operational use;
    - Encryption of all information on new laptop;
    - Research sources of training for systems security;
    - Investigate any electronic methods that may be used to locate the missing laptop;
    - Review and revise all physical security measures and retention schedule of clients' personal information.

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 JD Walls 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 JD Walls 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 interpreting the above referenced phrase, it is clear that in order for me to require that JD Walls notify individuals, there must be some harm – some damage or detriment or injury – that could be caused to the Organization'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] Although JD Walls reported that the type of harm that could result from the unauthorized access to personal information is identity theft, the Organization believed that the risk of identity theft was not that likely for the following reasons:

- The information was not the target of the theft; many other consumer items were stolen.

- …it appears the robber was looking for items that were easy to sell for some quick cash.
- The information could be used to commit fraud or identity theft; however it was stolen in the United States (Cathedral City, California) and contains Canadian information which would make it harder to apply for credit cards or loans. All the addresses (except for 4) were in Canada.
- There is no diagnostic, treatment and care information contained on the computer or the files stolen.

[13] In this case, the personal information at issue is of high sensitivity as it includes client name, home address, telephone numbers, birth date, email address, social insurance number, financial information included in the personal income tax returns, and spouse and dependent(s) names. The information is highly sensitive personal information and is of value to those who commit theft. The type of harm that could result from the unauthorized access to this personal information is identity theft, which, in my view is a significant harm.

[14] In order for me to require JD Walls to notify the affected individuals, however, there must also be a "real risk" of significant harm to its 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 harm in this case, I considered that the personal information at issue is sensitive in nature and could be used to commit identity theft. There were no security access controls to obtain access to personal information maintained on the laptop and hard disk backup. The Organization reported that the stolen personal information does not carry a high probability of identity theft for reasons that the information was not the intended target of the robbery, and it would be difficult to use "Canadian information" to apply for credit cards or loans in the United States. Notwithstanding the Organizations reasons why the stolen personal information does not carry a high risk of identity theft, the fact remains that the incident was committed by thieve(s) with malicious intent.

[16] My Office also contacted the Economic Crimes Section ("ECS") of the Edmonton Police Service as part of my investigation of this matter. ECS reviews and evaluates all complaints of fraud, false pretences, credit card offences, counterfeiting crimes, identity theft and perjury, and assists both Edmonton Police Service members and external agencies in the investigation of fraud-related crime.

[17] According to Detective Bob Gauthier of ECS, personal information of individuals regardless of which country it originated from is used, in most cases as a commodity amongst culprits. He went on to say that "stoolies" who have stolen a good amount of personal information are able to sell it on the black market to others who will ultimately

use it to commit fraud. “Chat rooms” or “Carder networks” are good examples of how thieves or “Carders” buy, sell, and trade online the personal information stolen from individuals or organizations. Given this information from ECS, I do not agree with JD Walls that since the theft occurred in the United States, Canadians will not be affected. The unprotected electronic files containing personal information on the laptop and hard disk can be easily transmitted around the globe.

[18] Given the information reported by JD Walls, 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 information at issue is of high sensitivity and could be used to commit identity theft; that the personal information on the laptop and hard disk backup were unencrypted; and, that even though the theft of the personal information of the laptop and hard disk may not have been the target of the theft, the thieves have ready access to the personal information stored on the laptop and the laptop has not been recovered.

V. Decision

[19] Based on the information reported to me by JD Walls, I have concluded that there is a real risk of significant harm to individuals as a result of this incident and I require JD Walls to notify 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 March 19, 2012 or such other date as I may specify.

Jill Clayton
Information and Privacy Commissioner