ALBERTA

OFFICE OF THE INFORMATION AND PRIVACY COMMISSIONER

P2011-ND-024

BEST BUY CANADA LTD.

July 19, 2011

(Case File #P1881)

I. Introduction

[1] On May 16, 2011, I received a report from Best Buy Canada Ltd. (the "Organization") of an incident involving the unauthorized access to or disclosure of personal information. Based on the information reported to me, I have decided that there is a real risk of significant harm to the individual involved as a result of the incident, and therefore I require that the Organization notify the individual 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 the 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 the 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 the 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 the 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) "the 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 the Organization 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 the Organization 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

[7] On May 16, 2011, I received a written report from the Organization describing an incident involving the unauthorized access to or disclosure of personal information.

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

- Customer A took a computer into the Edmonton West store for service.
- Customer B also had a computer in for service at the same location. When Customer B came to pick up his computer on May 9, 2011, Customer A's computer was released to Customer B in error.
- Customer A and B had the same first names and the Organization's employee mistakenly matched the names on the units and not the invoice number.
- Customer A came into the store on May 11, 2011, to pick up his computer and the error was discovered. The Organization's Manager contacted Customer B to advise him of the error that day and requested the return of Customer A's computer.
- Customer B returned Customer A's computer to the store on May 12, 2011, at which time the Organization had Customer B confirm in writing that Customer B had not copied, retained, or distributed the information on Customer A's computer.
- The type and amount of information on Customer A's computer was initially reported by the Organization as unknown. The Organization in a May 12, 2011,

letter to Customer A described the content of the hard drive as "recent data back up." After several attempts by the Organization and my Office to contact Customer A to determine the contents of the hard drive, Customer A sent an email to my Office on July 13, 2011. Customer A stated the hard drive contained financial information, including tax information and business and personal account information.

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

[9] Pursuant to section 37.1 of PIPA, I have the power to 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." In determining whether or not to require the Organization to notify individuals, I must consider whether there exists a "real risk of significant harm" to individuals as a result of the incident.

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

[11] In this case, the personal information at issue is of moderate to high sensitivity as tax and financial account information was contained on the hard drive. It was stated in the Organization's correspondence with Customer A that backup data was on the hard drive. This can include backup from the email system and personal documents.

[12] The Organization 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.

[13] In order for me to require the Organization to notify Customer A, however, there must also be a "real risk" of harm to the individual 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.

[14] In deciding whether there exists a "real risk" of harm in this case, I considered that the data elements pose a risk of identity theft and that Customer B returned the hard drive only after the error was discovered by the Organization and was asked to return the information.

[15] Given the information reported by the Organization and Customer A, I have decided that there is a real risk of significant harm to Customer A as a result of the incident as the data elements post a risk of identity theft, which is a significant harm. In arriving at this conclusion, I also considered that Customer B provided a written

representation that the information was not copied or distributed and that Customer B returned the hard drive after the Organization discovered the error.

V. Decision

[16] Based on the information reported to me by the Organization and Customer A, I have concluded there is a real risk of significant harm to Customer A as a result of this incident, and I require the Organization to notify Customer A in accordance with section 19.1 of the *Personal Information Protection Act Regulation*.

[17] I understand that the Organization has already notified Customer A by way of a letter sent by registered mail on May 19, 2011.

Frank Work, Q.C.
Information and Privacy Commissioner