Office of the Information and Privacy Commissioner of Alberta

PERSONAL INFORMATION PROTECTION ACT
Breach Notification Decision

Organization providing notice under section 34.1 of PIPA	Best Buy Canada Ltd.(Organization)
Decision number (file number)	P2014-ND-54 (File #P2375)
Date notice received by OIPC	July 10, 2013
Date Organization last provided information	October 18, 2013 and March 12, 2014
Date of decision	April 15, 2014
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the individuals pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is incorporated in Alberta. I have jurisdiction because the Organization is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	According to the Organization, the information believed to be at issue in this matter is the type of information typically found in word documents, videos, music, and photos stored on a personal computer. This information is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ❑ unauthorized access ☒ unauthorized disclosure	

Description of incident	• On June 26, 2013, the Organization sold a used computer to Customer B. • Customer B discovered personal information belonging to the son of the previous owner of the computer (Customer A) on its secondary hard drive. • On July 5, 2013, Customer B's father returned the computer to the Edmonton South store location. Customer B's father indicated that he copied the data on the computer onto a USB flash drive in order to provide it to the police. • The Organization did a cursory review of the computer's contents. The review showed the computer had files containing videos, music, photos, and word documents. • The Organization investigated and found that the Organization's service depot failed to identify and properly wipe the secondary hard drive prior to returning the computer to the store for resale. • The Organization notified Customer A of the incident on July 11, 2013 by couriered letter and telephone. • Customer A indicated that the computer belonged to her son. Customer A told the Organization that she felt none of the data was sensitive or important and was likely music and videos. • The Organization reported there is a possibility the computer may have been on the sales floor as a demonstration model with the personal information on it before it was sold to Customer B. • The Organization deleted the information that was on the computer and cannot say with certainty what personal information was on the computer.
Affected individuals	One individual: Customer A's son.
Steps taken to reduce risk of harm to individuals	• Customer B returned the computer and provided the USB flash drive to the Organization. • The Organization obtained a written undertaking from Customer B confirming the personal information was not copied, retained or disclosed further. • The Organization wiped the computer and destroyed the USB flash drive.
Steps taken to notify individuals of the incident	• The Organization notified Customer A on July 11, 2013 via couriered letter and telephone. • The Organization provided Customer A with an update on the resolution of this incident on September 9, 2013.

REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury – that could be caused to those affected individuals as a result of the incident. The harm must also be "significant." It must be important, meaningful, and with non-trivial consequences or effects.	The Organization reported that, due to the nature of the information involved and its conversations with Customer A, it believed the potential harm to the affected individual was low. In circumstances where there is no exact inventory of personal information available from either the Organization or the affected individual, it is impossible to evaluate the sensitivity of the personal information on the computer. However, from the Organization's report of this matter, the information believed to be at issue is the type of information typically found in word documents, videos, music, and photos stored on a personal computer. In my view, this type of information could be used to cause the harms of hurt and humiliation, which are significant harms.
Real Risk The likelihood that the significant harm will result must be more than mere speculation or conjecture. There must be a cause and effect relationship between the incident and the possible harm.	The Organization submitted that the risk of harm was low for the following reasons: • Customer B's father alerted the Organization of the error. • Customer B returned the computer and the USB flash drive that contained a data copy to the Organization. • Customer A's data was not encrypted or password protected; however, Customer B works for a law enforcement agency so it is unlikely that Customer B would use the data for fraudulent purposes. • It is "unlikely" that the computer was on the sales floor as a demo model. Although it is technically possible for someone to find the secondary drive, it is highly unlikely given how customers typically interact with demonstration computers. • The incident is a result of human error and not malicious intent. In my view, the likelihood of harm resulting from this incident is increased because the organization did not perform a thorough inventory of the contents of Customer A's computer when it was returned. This means the Organization cannot say with certainty that the computer did not contain more sensitive personal information. Further, the Organization identified the possibility that the computer was displayed on the sales floor before it became aware of this incident. The Organization cannot say with certainty whether the computer was on the sales floor, leaving a residual risk that information on the computer may have been accessed by another customer.

DECISION UNDER SECTION 37.1(1) OF PIPA
Based on the information provided by the Organization and given the circumstances of the incident, I have decided that there is a real risk of significant harm to the affected individual. The factors which contributed significantly to my decision are as follows: 1) no one can confirm exactly what personal information was on the computer; 2) there is a possibility that the computer containing the personal information may have been on the sales floor as a demonstration model before it was sold to another individual. I require the Organization to notify the affected individual in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) I understand the Organization notified the affected individual by letter and phone call on July 11, 2013, in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner