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)	P2018-ND-166 (File #010289)
Date notice received by OIPC	October 31, 2018
Date Organization last provided information	October 31, 2018
Date of decision	December 14, 2018
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 operates in Alberta and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involves a missing form and hard drive. The form included customer contact information (address, telephone number) and signature. The Organization reported the affected customer said that the missing hard drive contained: • family pictures, • business documents, • personal information of customer's clients. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On or around August 24, 2018 the Organization sent a customer's hard drive to a third party data recovery company. • The hard drive was lost in transit, along with a copy of an in-store sign-in form which is used to record the terms and details of the requested service and the customer's information. • The incident was discovered on October 3, 2018. • The hard drive and form have not been recovered.
Affected individuals	The Organization reported the incident presents a real risk of significant harm to one individual and the Organization's customer's clients.
Steps taken to reduce risk of harm to individuals	Offered 12 months free credit monitoring to the customer.
Steps taken to notify individuals of the incident	The customer was contacted by telephone on October 23, 2018 and October 26, 2018. The Organization reported that "A formal letter will be sent to our customer shortly to provide her with additional information concerning the free 12 months credit monitoring service."
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to 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: *The information available on the Form, in particular, a customer's signature, along with that customer's name and adress [sic] could provide a foundation for identity thieft/fraud [sic].* *If the data on the hard drive is ever retrieved or accessed by a third party, it could potentially cause:* *Financial loss, fraud and identity thieft [sic].* I accept the Organization's assessment that the information on the form (contact information and signature), along with knowledge of the customer's relationship with the Organization, could be a foundation for identity theft and fraud. Based on the Organization's report, information on the hard drive could be used to cause the harms of identity theft, fraud and financial loss. These 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 reported: • "The loss of this hard drive and the Form is the result of a human error and we don't believe that there is any malicious intent." • "We believe the risk of harm is significant, the location of the hard drive and the Form is unknown. The hard drive and the Form have been missing since August 24, 2018." • "It is unlikely that the data on the hard drive will be accessed as the hard drive was defective and was sent to [the data recovery company] to attempt a data recovery. However if the data is ever retrieved or accessed by a third party, the sensitivity could be high." • "We were informed by our customer that the hard drive did contain some of her business documents and the personal information of some of her clients." In my view, a reasonable person would consider there is a real risk of significant harm resulting from this incident. The hard drive has not been recovered, and the Organization cannot know if it is misplaced or stolen. The hard drive was being sent for attempted data recovery, which suggests it may be possible to access the data.

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 individuals.

I accept the Organization's assessment that the information on the form (contact information and signature), along with knowledge of the customer's relationship with the Organization, could be a foundation for identity theft and fraud. Based on the Organization's report, information on the hard drive could be used to cause the harms of identity theft, fraud and financial loss. These are significant harms.

The hard drive has not been recovered, and the Organization cannot know if it is misplaced or stolen. The hard drive was being sent for attempted data recovery, which suggests it may be possible to access the data on the hard drive

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand that the customer was contacted by telephone on October 23, 2018 and October 26, 2018 and will receive a formal letter. The Organization is not required to notify the customer again.

I note, however, that the Organization reported "The affected customer alleged that the hard drive contained … Some of her clients' personal information".

The requirement in section 34.1 of PIPA to report incidents to me applies to "An organization having personal information under its control….". In this case, it appears the Organization may have had control of personal information about clients of the Organization's customer, although this is not entirely clear. Nonetheless, this breach notification decision applies to the Organization in respect of personal information (about identifiable individuals) in its control.

To the extent this incident involves personal information in the control of another organization (or public body or custodian that may be subject to Alberta's privacy laws other than PIPA), I require the Organization to notify that other entity about this incident, and provide a copy of this breach notification decision, as that other entity may have obligations to report this incident to me, and to notify affected individuals.

I require the Organization to confirm to my office in writing within ten (10) days of the date of this decision that it has complied with this decision.

Jill Clayton
Information and Privacy Commissioner