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	London Drugs Ltd. (Organization)
Decision number (file number)	P2018-ND-026 (File #007538)
Date notice received by OIPC	January 19, 2018
Date Organization last provided information	January 19, 2018
Date of decision	February 5, 2018
Summary of decision	There is a real risk of significant harm to the individual affected by this incident. The Organization is required to notify the individual in Alberta pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA).
JURISDICTION	
Section 1(1)(i) of PIPA "organization"	The Organization is an "organization" as defined in section 1(1)(i) of PIPA. This incident involves theft of a customer's laptop computer, while the computer was with the Organization for servicing. OIPC Order P2010-008 considered a similar situation and found the organization in that case had custody of personal information stored on the computer. In this case, in my view, the Organization had both custody and control of the personal information at the time of the incident, and therefore an obligation to report this matter to me under section 34.1 of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization reported "Specific details of the personal information are unknown …We understand that the computer was used for personal purposes of the customer, rather than business. Included on the computer was miscellaneous files and digital images." Further, "The laptop computer contained personal data of the customer." The Organization reported the information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. The incident took place in Alberta.

DESCRIPTION OF INCIDENT	
☒ loss ❑ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On January 12, 2018, just before store closing, a customer's laptop computer, which was being serviced by technicians, was stolen from a non-public (employee only) tech room, while the room was temporarily vacant. • The incident was discovered the same day when an employee noticed the laptop was missing. In-store video footage confirms the laptop was stolen by another customer.
Affected individuals	The incident affected one (1) resident of Alberta.
Steps taken to reduce risk of harm to individuals	• Reported the incident to law enforcement. • Advised customer to take steps to protect against identity theft and fraud and recommended that passwords be changed, and to notify financial institutions. • Offered to pay for one year of credit monitoring service for affected individual.
Steps taken to notify individuals of the incident	Notified affected individual by telephone on January 13, 2018.
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 "Included on the computer was miscellaneous files and digital images" and "The customer did not believe he had any particularly sensitive data on the computer when asked. However, [the Organization] does not know the specific nature of that data and it is possible some information could be sensitive." In terms of potential harms that might result from this incident, the Organization reported "Aside from the lost laptop, there is potential misuse of customer's personal data that was on the computer" and also "If any of the data is sensitive, there is a risk it could be used for criminal or improper purposes, such as identity theft or fraud." In a previous breach notification decision (P2014-ND-054), I said "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." In this case, given the Organization's report that the computer contained "miscellaneous files and digital images", I similarly find that the information could be used to cause the harms of hurt and humiliation, which are significant harms. I also agree with the Organization that "If any of the data is sensitive, there is a risk it could be used for criminal or improper purposes, such as identity theft or fraud."
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 "Because the laptop was stolen, which is evidence of malicious intent, there is reasonable likelihood of harm, depending on the nature of the data (which we do not have knowledge of)." I agree with the Organization. The incident was the result of malicious intent (theft), and the information has not been recovered.

DECISION UNDER SECTION 37.1(1) OF PIPA

Given the information reported by the Organization, and considering the circumstances in this case, I have decided that there is a real risk of significant harm to the affected individual.

The Organization reported that the computer contained "miscellaneous files and digital images". In my view, this information could be used to cause the harms of hurt and humiliation, which are significant harms. I also agree with the Organization that "If any of the data is sensitive, there is a risk it could be used for criminal or improper purposes, such as identity theft or fraud." The incident was the result of malicious intent (theft), and the information has not been recovered.

The Organization is required to notify the affected individual in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individual by telephone on January 13, 2018. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner