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 Limited (Organization) |
| **Decision number (file number)** | P2019-ND-098 (File #012499) |
| **Date notice received by OIPC** | March 18, 2019 |
| **Date Organization last provided information** | March 18, 2019 |
| **Date of decision** | July 16, 2019 |
| **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 Organization reported the information at issue may include:<br>• photos,<br>• social insurance number,<br>• mortgage documents, and<br>• banking information.<br><br>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 around March 13, 2018, a customer notified the Organization that she found data on her hard drive belonging to another customer. The customer notified the other customer directly about the data disclosure. |

| | |
|---|---|
| | • Both customers had brought their computers to the Organization for servicing.<br>• The Organization is investigating, but suspects that when the service technician copied the data over to the store's encrypted hard drive for storage, he failed to subsequently clear data off the encrypted hard drive upon completion of that service work.<br>• The incident is believed to have occurred between December 29, 2018 and January 2, 2019. |
| **Affected individuals** | The incident affected 2 individuals. |
| **Steps taken to reduce risk of harm to individuals** | • Requesting return of the hard drive in possession of the unauthorized recipient so it can be secured and wiped.<br>• Requesting confirmation that the unauthorized recipient has not retained any copy of any personal information.<br>• Conducting an internal investigation.<br>• Will offer the affected individual credit monitoring protection.<br>• Reviewing policies and procedures with applicable employee(s), along with counselling and/or disciplinary measures as appropriate. |
| **Steps taken to notify individuals of the incident** | The Organization reported that it will be meeting with the affected individual, but that notification has not yet happened. |
| **REAL RISK OF SIGNIFICANT HARM ANALYSIS** | |
| **Harm**<br>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 possible harm will depend on precise nature of personal information that was disclosed, which we do not have direct knowledge of. But to extent [sic] it includes sensitive personal information as advised, the customer could be harmed through its misuse including, but not limited to, being at risk for identify theft."<br><br>I accept the Organization's assessment. A reasonable person would consider that the personal information at issue could be used to cause the harms of fraud and identity theft. These are significant harms. |
| **Real Risk**<br>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:<br><br>*We have no reason to believe that Customer B, who brought this matter to our attention as well as to the attention of Customer A, would retain Customer A's information or use it for any improper purpose. Customer B is being asked to return the hard drive with Customer A's information to ensure it is appropriately wiped and to not retain any copies of Customer A's information.* |

| | |
|---|---|
| | *Our investigation will help to determine if there is any possible risk that Customer A's information could have been disclosed to any other customers. We have no evidence or reason to believe that occurred in this instance, but if it were to have occurred [sic], the likelihood of harm would increase.*<br><br>In my view, the likelihood of significant harm resulting in this case is decreased because the incident resulted from human error and not malicious intent, and the unauthorized recipient reported the breach to the Organization. However, the Organization has not recovered the hard drive, and has not yet confirmed that the personal information was not disclosed, copied or saved. |

**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.

A reasonable person would consider that the personal information at issue could be used to cause the harms of fraud and identity theft. These are significant harms. The likelihood of significant harm resulting in this case is decreased because the incident resulted from human error and not malicious intent, and the unauthorized recipient reported the breach to the Organization. However, the Organization has not recovered the hard drive, and has not yet confirmed that the personal information was not disclosed, copied or saved.

**The Organization is required to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) and confirm to me in writing, within 10 days of the date of this decision, that it has done so.**

Jill Clayton
Information and Privacy Commissioner