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	Monkey Business Day Homes Inc. (Organization)
Decision number (file number)	P2015-ND-09 (File #P2925)
Date notice received by OIPC	November 21, 2014
Date Organization last provided information	January 14, 2015
Date of decision	March 9, 2015
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify those 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).
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information about the individuals: • name; • address; • phone number; • email address; • children pick-up and drop-off times; • emergency contact information; • SIN numbers; • criminal record checks; and • employee payslips. This information is "personal information" as defined in section 1(1)(k) of PIPA and was collected in Alberta.

DESCRIPTION OF INCIDENT	
☒ loss ☐ unauthorized access ☐ unauthorized disclosure	
Description of incident	• On October 17, 2014, a laptop was stolen from the Organization's unlocked premises. • The laptop was password protected but not encrypted. • The laptop contained personal information about children who attend the day home, their parents and staff members.
Affected individuals	Twelve (12) individuals were affected, including families and staff members.
Steps taken to reduce risk of harm to individuals	• Reported incident to Medicine Hat Police. • Reported incident to Children Family Services Alberta.
Steps taken to notify individuals of the incident	Affected parents, providers and staff were notified by phone on October 22, 2014. A note was also written on the October invoices sent to parents.
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 recognized the affected individuals may be at risk for identity theft, fraud and loss of property. In my view, the personal information involved is highly sensitive. It includes names, addresses, telephone numbers, email addresses, child pick-up and drop-off times, emergency contact information, SIN numbers, criminal record checks and employee payslips. The types of harm that could result from this incident are identity theft/fraud, humiliation (in regards to information on criminal record checks), and possibly physical harm to a vulnerable population (children). In my view, 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 a moderate risk of significant harm to the affected individuals due to the sensitivity of the personal information involved. In my view, there is a real risk of significant harm resulting from this incident. The likelihood of harm is increased because the incident was the result of malicious intent (stolen laptop). The laptop was password protected but not encrypted, and has not been recovered.

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. The personal information involves sensitive personal information, such as SIN numbers and employee payslip information as well as employee criminal record checks. It also includes the drop-off and pick-up times and addresses of the children attending the day home. The information was stolen, which increases the risk of information being used for an unlawful purpose. The laptop was not encrypted which increases the ease with which the information could be accessed and the laptop has not been recovered. These factors contributed significantly to my decision. 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 the Organization notified the affected individuals in a letter dated February 27, 2015 in accordance with the Regulation. The Organization is, therefore, not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner