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	CBI Home Health (AB) Limited Partnership (Organization)
Decision number (file number)	P2017-ND-97 (File #000122)
Date notice received by OIPC	January 14, 2015
Date Organization last provided information	July 6, 2016
Date of decision	August 30, 2017
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 operates in Alberta and provides home care services. Given this, I considered whether or not Alberta's *Health Information Act* (HIA) applies in this case as, pursuant to section 4(3)(f), PIPA does not apply to "health information" as defined in HIA to which that Act applies. The Organization reported that the information at issue in this matter is personal employee information from its scheduling software. Based on this, and considering the Organization is not an "affiliate" or a "custodian" under the HIA, the HIA does not apply. Nonetheless, the Organization is a limited partnership and qualifies as an "organization" as defined in section 1(1)(i)(iv) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information: • name, • address, • telephone number (cell and home), • seniority list (including total hours worked), • hourly pay rates.

	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	• The Organization reported that, between mid-November and December 17, 2014, an employee responsible for recruitment, with authorized access to the Organization's scheduling software database, accessed and ran a number of human resource reports without a legitimate business purpose. • These reports contained personal employee information of the Organization's employees. • Shortly thereafter, the Organization received complaints from approximately five to ten employees who claimed that individuals identifying themselves as union representatives had arrived at their homes and knew details of the information at issue. Some employees reported receiving repeated telephone calls from union representatives. At the time, the workplace was not yet unionized. • The Organization concluded that the employee had disclosed the information at issue to the union. • The information in the human resource reports has not been recovered.
Affected individuals	The incident affected a total of 530 individuals, including 529 employees and one (1) client.
Steps taken to reduce risk of harm to individuals	• Restricted access to employee lists and employee reports from its scheduling software and reduced the amount of personal information it contains. • The employee is no longer employed at the Organization.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter sent on December 19, 2014.

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 that "There is low to medium potential of humiliation and/or damage to reputation or relationships as employee's pay rates were obtained. Employees have reported to us that the [union] representatives have accurately reported their current salaries and date of hires to them. There is low potential for damage to loss or loss [sic] of property where an individual's name is connected to his or her home address. The level of sensitivity for this breach and the risk of harm are low with respect to employees' name, address and phone numbers were [sic] in the lists. There is low risk of identity theft or financial loss. SINs were not on the list." The Organization also reported that "Some of the [Organization's] employees have expressed … that they felt intimidated as a result of [the union's] use of their personal information" and later that many employees "are immigrants from other countries and backgrounds that make it even more likely that they will be intimidated and concerned when approached in this matter." In assessing the possible harms that might be caused to affected individuals as a result of this incident, I note that the Organization does not know with certainty that the information at issue was provided to the union. Should any harm result, the Organization is speculating that it is the result of this incident. That said, in my view, the contact information at issue could be used to send unsolicited letters, or make telephone calls or in-person visits. While I accept the Organization's assessment that such contact could cause stress for some individuals (irrespective of their citizenship and background), I am not persuaded that this is a significant harm. The union representatives' in-person and/or telephone interactions with the affected individuals are, in my view, non-threatening forms of contact and can be dealt with by closing the door, and hanging up the telephone. These interactions do not rise to the level of causing significant damage or detriment or injury. It is also possible that contact information could be used for phishing purposes, or to cause damage to or loss of property. These are significant harms. However, it is unlikely that these harms will result in this case, for reasons discussed below. The employment information at issue could possibly be used to cause hurt, humiliation, embarrassment or damage to reputation and relationships, particularly if the information is shared with individuals who have personal or professional relationships with the affected individuals. These are significant harms.

	I also agree with the Organization that it is unlikely the information could be used for identity theft or fraud, and, for reasons discussed below, I find it is unlikely the information would be used for this purpose.
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.	In assessing the likelihood that harm would result from this incident, the Organization initially listed a number of factors that it considered as follows: • "A former employee obtained access to the information." • "The employee lists were password protected at the time of the privacy breach." • "Some of the information may be highly sensitive (ie. Salary /pay rate information)." • "The information has been exposed since mid-November 2014." • "There is evidence of a malicious intent or purpose in providing the information to … assist in union organizing efforts." • "The information could be used for identity theft or fraud, although the risk is low." • "The information was not recovered." • "529 employees were affected by the breach." • "No vulnerable individuals were involved." The Organization later reported that it had changed its assessment to a "real risk of significant harm" noting a specific individual's complaint that she was contacted by a union representative who asked to speak with her home care aid (an employee of the Organization). The Organization stated that the "only reasonable inference is to be drawn from these circumstances is that the union representative obtained the client's contact information through [the Organization]". I considered the Organization's comments, and note that the Organization did not provide evidence that the contact described was the result of this incident, but rather speculated that this was the case. In any event, I have already said that simply being contacted by the union is not, in itself, a significant harm.

	I also said that use of the information for phishing purposes, or to cause damage to or loss of property, or for identity theft or fraud, would be significant harms. However, the circumstances as reported by the Organization suggest the information was disclosed to the union for the specific purpose of enabling union representatives to contact employees to persuade them to unionize. There is no suggestion that union representatives attempted to masquerade as, nor impersonate, any other entity, and did not try to mislead the affected individuals. Given these circumstances, I find it unlikely that the information would be used to cause any of these significant harms. The employment information at issue could be used to cause the harms of hurt, humiliation, embarrassment or damage to reputation and relationships, particularly if the information is shared with individuals who have personal or professional relationships with the affected individuals. From information reported by the Organization, it appears that these harms may have already occurred.

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 contact information at issue could be used to send unsolicited letters, or to make telephone calls or in-person visits; however, in the circumstances, I have decided these are not significant harms. The same information could also be used for phishing purposes, or to cause damage to or loss of property. While these are significant harms, the circumstances as reported by the Organization suggest the information was disclosed to the union for the specific purpose of enabling union representatives to contact employees to persuade them to unionize. There is no suggestion that union representatives attempted to masquerade as, nor impersonate, any other entity, and did not try to mislead the affected individuals. Given these circumstances, I find it unlikely that the information would be used to cause any of these significant harms.

Despite the above, in my view, the employment information at issue could be used to cause the significant harms of hurt, humiliation, embarrassment or damage to reputation and relationships, particularly if the information is shared with individuals who have personal or professional relationships with the affected individuals. From information reported by the Organization, it appears that these harms may have already occurred.

Given this, I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). The Organization reported that it notified affected individuals by letter sent on December 19, 2014. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner