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	Lawson Products, Inc. (Organization)
Decision number (file number)	P2019-ND-022 (File #010666)
Date notice received by OIPC	November 15, 2018
Date Organization last provided information	November 15, 2018
Date of decision	February 15, 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 whose personal information was collected 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.
Section 1(1)(k) of PIPA "personal information"	The incident involved the following information for one affected individual: • name, email address and bank account information (including full routing numbers) The following information was at issue for three individuals: • name, gross sales and commission compensation for the years 2001 to 2014. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization determined that an email account was compromised and an unknown person gained access to the contents of the email account. • Forensic investigation was able to determine which email messages in that account were affected. Two such messages contained personal information related to residents of Alberta, most all of whom are commissioned sales contractors and one a commissioned sales employee for the Organization. • The incident occurred between October 1-2, 2018 and was discovered on October 2, 2018 when various employees noticed unusual messages being sent from the compromised email account and reported it to the Organization's IT department.
Affected individuals	The incident affected 15 individuals, 4 of whom are residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Continues to educate employees regarding the risk associated with phishing. • Employees are instructed to not use email to communicate sensitive information, such as banking information. • Implementing two factor authentication, which should significantly reduce the risk of account takeovers associated with phishing.
Steps taken to notify individuals of the incident	The Organization notified the affected individual whose bank account information was at issue. The sales contractors were not notified.
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 "Compromise of a person's name and bank account particulars may result in fraud" and "Compromise of a person's sales performance and commission compensation may affect the individual's reputation. Given that sales performance is generally well-known within the company, we have concluded that this is unlikely." In my view, a reasonable person would consider that name, email address and financial information could be used to cause the significant harms of identity theft and fraud, as well as phishing (leading to an increased risk of fraud or identity theft). Information related to sales performance and commission compensation could be used to cause hurt, humiliation, and embarrassment and could result in damage to reputation. These are all 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 that "These emails were accessed by an individual or individuals who used phishing to compromise the email account in question and accessed these emails without authorization. This suggests a malevolent intent, increasing the risk of harm." As noted above, the Organization also reported "Compromise of a person's sales performance and commission compensation may affect the individual's reputation. Given that sales performance is generally well-known within the company, we have concluded that this is unlikely." I agree with the Organization's assessment in part. A reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (phishing). However, although sales performance activity may be "generally well-known within the company", it is impossible to know how the unauthorized individual(s) will use or disclose the information.

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 name, email address and financial information could be used to cause the significant harms of identity theft and fraud, as well as phishing (leading to an increased risk of fraud or identity theft). Information related to sales performance and commission compensation could be used to cause hurt, humiliation, and embarrassment and could result in damage to reputation. These are all significant harms. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (phishing). However, although sales performance activity may be "generally well-known within the company", it is impossible to know how the unauthorized individual(s) will use or disclose the information.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individual whose bank account information was at issue. The Organization is not required to notify this individual again. However, sales contractors were not notified. **The Organization is required to confirm to my office in writing within 10 days of the date of this decision that the affected individuals whose personal information was collected in Alberta have been notified in accordance with the Regulation.**

Jill Clayton
Information and Privacy Commissioner