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	La Coop fédérée (Organization)
Decision number (file number)	P2018-ND-083 (File #008650)
Date notice received by OIPC	May 9, 2018
Date Organization last provided information	May 9, 2018
Date of decision	July 17, 2018
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 an agricultural business based in Quebec and is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involves the following information: • name, • title, • postal code, • date of birth, • start date with the organization, • annual salary, • bonus consideration, and • information about the type of benefit plan they participate in. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was in an email attachment containing personal information for about 73 employees of a then third-party company, which has since been acquired by the Organization and is now a wholly-owned subsidiary, located in three different provinces (AB, SK, MB).

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On March 5, 2018, the Organization received a phishing email from a company that had an existing business relationship with the Organization. The company had itself been compromised. • The phishing email was primarily blocked by the Organization's anti-spam filter; however, one (1) user who received the email clicked the link displayed and several emails were sent from his mailbox leading three recipients to also click the link and provide their authentication information. • Three email accounts were ultimately compromised. • Approximately 2,500 emails were sent from the compromised email accounts and the hacker had the ability to access a limited amount of personal information inside those accounts, including an email attachment containing the information at issue. • There is no evidence the attachment was opened, downloaded or transferred during the attack. • The Organization advised affected individuals that it became aware on March 14, 2018 that an unauthorized person may have accessed the personal information.
Affected individuals	The incident affected a total of 73 individuals, including 17 in Alberta.
Steps taken to reduce risk of harm to individuals	• Retained an external consultant to assist in incident response including email analysis, hard drive analysis, firewall log analysis and VPN access log analysis. • The Organization reported that immediate steps were taken to contain and reduce the harm of the breach including changing the passwords, blocking the IP address within the firewall, monitoring extensively to see if there were any further intrusions. • All employees were notified not to respond to any emails that they receive from the three compromised email Outlook accounts. • The then third-party company whose employees were listed on the compromised spreadsheet was notified on March 21, 2018. • The Organization will take steps with employees to refresh training in respect of phishing emails and will continue its strategy of ensuring staff training, audits, supervision strategies and technical security architecture.
Steps taken to notify individuals of the incident	The Organization notified employees on or around April 20, 2018.

REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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 were no email addresses compromised, so the risk of phishing to the employees is relatively low. However, their birthdates were available. There is limited risk that birthdate can be used for identity theft…". I agree with the Organization's assessment. The contact, identity and employment information at issue could be used to cause the significant harms of identity theft and 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 "Given that the action arose from the malicious action of an unknown third person through deliberate intrusion, the likelihood of harm is increased." I agree with the Organization. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion) and approximately 2,500 unauthorized emails were generated, which may have been sent to cause harm to recipients. It appears the information may have been exposed for over a week before the Organization became aware of the risk to personal 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 as a result of this incident.

The contact, identity and employment information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion) and approximately 2,500 unauthorized emails were generated, which may have been sent to cause harm to recipients. It appears the information may have been exposed for over a week before the Organization became aware of the risk to personal information.

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

I understand the Organization notified employees on or around April 20, 2018. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner