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	Civeo (Civeo Services Employees LP) (Organization)
Decision number (file number)	P2018-ND-140 (File #010155)
Date notice received by OIPC	October 24, 2018
Date Organization last provided information	November 5, 2018
Date of decision	November 14, 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 individuals whose 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: • social insurance number, • driver's license image, and • copy of void check. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The Organization reported the information was collected in Alberta.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization reported that "Employees responded to phishing email resulting in compromise of email accounts".

	• In its notification to affected individuals, the Organization said the incident "occurred between October 4 and October 10, 2018. Unknowingly, 14 employees responded to a Phishing email scheme that resulted in a compromise of their email id and password. An unknown party, located in Egypt, had access and logged into these 14 employees [sic] email accounts and that access ranged from one day to five days. Our investigation determined that the unknown party did not copy email out of these email accounts, however, the unknown party did have view access [sic] these email accounts." • The breach was discovered on October 2, 2018 via suspicious login geography by the Organization's Cyber Security team.
Affected individuals	The incident affected 23 individuals.
Steps taken to reduce risk of harm to individuals	• Made employees aware via notification to them. • Offered information on how to obtain free credit reporting and also indicated that the Organization will pay for three months monitoring for active employees. • Enhanced end user awareness training. • Evaluating email retention policy and practices. • Reported breach to State of Louisiana Attorney General.
Steps taken to notify individuals of the incident	Affected individuals were notified by email sent October 19, 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 "Information could be used to attempt identity related thefts". I agree with the Organization's assessment. The identity and financial 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.	In assessing the likelihood of harm resulting from this breach, the Organization reported "The perpetrator attempted to submit ficticious [sic] invoices for payment to a vendor and bank account under his control. He did not copy email out of our system, so data at risk would have been for a short period of time and via display only. For this reason, we suspect there to be a low risk that harm will result."

	In my view, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (phishing). The unauthorized party had access for up to 5 days and made attempts to use information for fraudulent purposes. The Organization reported the unauthorized party did not copy email from the system; however, there is no way to confirm the unauthorized party did not copy the information in some form.

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 identity and financial 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 (phishing). The unauthorized party had access for up to 5 days and made attempts to use information for fraudulent purposes. The Organization reported the unauthorized party did not copy email from the system; however, there is no way to confirm the unauthorized party did not copy the information in some form.

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

I understand that affected individuals were notified by email sent October 19, 2018. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner