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	Westcorp Inc. (Organization)
Decision number (file number)	P2018-ND-112 (File #008173)
Date notice received by OIPC	March 29, 2018
Date Organization last provided information	May 3, 2018
Date of decision	August 13, 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 operates in Alberta and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • employee name, • driver's license number, • social insurance number, • banking information, and • credit card information. 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	• On June 23, 2017, the Organization's IT department became aware of a cyberattack on its servers. • The attack encrypted the network and compromised the functionality of the Organization's systems, including its redundant backups. The attackers demanded a ransom payment to unencrypt the affected files.

	• On June 26, 2017, the virus was contained, email functionality restored, and telephone lines temporarily forwarded to alternate numbers. Restoring software functionality took more time.
Affected individuals	The incident affected approximately 446 individuals.
Steps taken to reduce risk of harm to individuals	• Recommended that staff change their personal passwords. • Upgraded Trend Micro to the latest version. • Installed new back-up system for software. • Added additional virus protection on computers. • Added additional security to email. • Provided security awareness training to all staff. • Reported incident to the Real Estate Council of Alberta and law enforcement.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on June 26, June 28 and July 7, 2017.
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 "Our hotels were unable to function, we had no functionality through any of our operating software. We were being held ransom, so it seems as though the damage is purely financial loss to [the Organization]." In my view, a reasonable person would consider that the identity and financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss to the affected individuals.
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 "We have no evidence to suggest personal information had been misappropriated, however, it is a possiblity [sic] and we have recommended to staff to change any personal password." The Organization also said that the "Harm is low. A consulting company did some monitoring on the dark web for weeks after the breach and nothing was discovered." In my view, 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 (deliberate intrusion and installation of ransomware). As noted above, the Organization reported that misappropriation is a possibility. The lack of reported incidents of identity theft or fraud to date is not a mitigating factor in the likelihood of harm resulting from this incident, as identity theft and fraud can happen months and even years after a data breach.

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 the identity and financial information at issue could be used to cause the significant harms of identity theft, fraud and financial loss. 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 (deliberate intrusion and installation of ransomware). The Organization reported that misappropriation is a possibility. The lack of reported incidents of identity theft or fraud to date is not a mitigating factor in the likelihood of harm resulting from this incident, as identity theft and fraud can happen months and even years after a data breach. 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 affected individuals in emails on June 26, June 28 and July 7, 2017 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner