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	Klondike Insurance Agencies Ltd. (Organization)
Decision number (file number)	P2023-ND-016 (File #029663)
Date notice received by OIPC	March 24, 2023
Date Organization last provided information	April 14, 2023
Date of decision	April 24, 2023
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 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 all or some of the following information: • name, • address, • driver's licence number, • driver's abstract report, • insurance history record, • 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. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• At the time of the incident, the Organization obtained information technology (IT) services, including cloud hosting, from a third party, Sandbox West Cloud Services Inc. (Sandbox). • On or about February 11, 2023, Sandbox was victim to a ransomware attack. Sandbox first notified the Organization on February 12, 2023. • On March 19, 2023, Sandbox provided the Organization with supplemental information; a letter confirmed "threat actors" conducted a "ransomware attack" and advised all "customers" about the potential for "a data breach." • On April 6, 2023, the Organization reported unsuccessful attempts to obtain details from Sandbox about the incident, including whether or not personal information was accessed without authorization, or exfiltrated.
Affected individuals	The incident affected "up to 7,000 people."
Steps taken to reduce risk of harm to individuals	• Migrated to a new service provider. • Implemented additional administrative and technical safeguards.
Steps taken to notify individuals of the incident	Affected individuals were not notified of the incident.
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: *Base on information provided on the OIPC Alberta website - if this personal information is stolen or copied and disclosed to a criminal third party - it could assist in identification theft. There may also be some risk of monetary theft and/or fraud resulting from compromised financial information.* I accept the Organization's assessment. A reasonable person would consider that name, address, driver's licence number, driver's abstract, insurance history, banking and credit card information could be used to cause the harms of identity theft, fraud, and possibly embarrassment, hurt or humiliation. These are 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	The Organization did not provide an assessment of the likelihood that harm will result. On April 6, 2023, the Organization explained: *We are not experts and given the circumstances cannot assess the potential risk of significant harm or likelihood of occurrence...*

possible harm.	*[There] has been no demand for ransom, no provision of encryption keys, no confirmed communications with a threat actor, and no malware found in restored ... applications – any of which might help [the Organization] confirm the nature of the outage...* *As described above and limited to the letter from Sandbox (March 19) - we have essentially no substantive information confirming whether or not any information was accessed...* *Given the circumstances and available information, it is impossible for Klondike Insurance to rule out "with certainty" the possibility that personal information was accessed and/or exfiltrated. It is also impossible to conclude "with certainty" that it has been accessed. Further, we do not know with certainty if there is a "threat actor". None was confirmed...* In my view, a reasonable person would consider that the likelihood of harm resulting from this incident is increased because the personal information was potentially compromised due to the reported malicious action of a threat actor (deliberate intrusion and deployment of ransomware). The letter received from Sandbox on March 19, 2023, confirmed "threat actors" conducted a "ransomware attack" and advised all "customers" about the potential for "a data breach." The Organization could not rule out the possibility of unauthorized access nor exfiltration of personal information. The ability for an Organization or their vendor to recover from a cybersecurity incident (ransomware) does not preclude the possibility that such an incident occurred, nor does it mitigate the risk of harm.

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.

Name, address, driver's licence number, driver's abstract, insurance history, banking and credit card information could be used to cause the harms of identity theft, fraud, and possibly embarrassment, hurt or humiliation. These are significant harms.

The likelihood of harm resulting from this incident is increased because the personal information was potentially compromised due to the reported malicious action of a threat actor (deliberate intrusion and deployment of ransomware). The letter received from Sandbox on March 19, 2023, confirmed "threat actors" conducted a "ransomware attack" and advised all "customers" about the potential for "a data breach." The Organization could not rule out the possibility of unauthorized access nor exfiltration of personal information. The ability for an Organization or their vendor to recover from a cybersecurity incident (ransomware) does not preclude the possibility that such an incident occurred, nor does it mitigate the risk of harm.

The Organization is required to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation) and is required to confirm to my Office, within ten (10) days of the date of this decision, that affected individuals have been notified of this incident in accordance with the requirements outlined in the Regulation.

If the Organization is unable to notify affected individuals under section 19.1(1), it may consider making a submission to my office pursuant to section 19.1(2) of the Regulation within seven (7) days of this decision. The submission must include reasons why direct notification is unreasonable in the circumstances and include a plan on how it intends to notify affected individuals indirectly.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance