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	SLR Consulting Ltd. (Organization)
Decision number (file number)	P2021-ND-297 (File #020686)
Date notice received by OIPC	April 14, 2021
Date Organization last provided information	April 14, 2021
Date of decision	March 2, 2022
Summary of decision	There is a real risk of significant harm as a result of this incident. The Organization is required to notify the individual 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"	SLR is an environmental consultancy firm with offices in Europe, Asia-Pacific, Africa, Canada and the USA. It operates business-to-business ("B2B") as opposed to business-to-consumer ("B2C"). The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident may have involved all or some of the following information about a resident of Alberta: • name, • address, • SLR Shareholding Information (Number, Value, Share Type), • bank account holder name(s), • bank name, and • bank account number and sort-code. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On February 28, 2021, the Organization was alerted to a ransomware attack on its systems, which encrypted its file servers, and ERP system in Europe and Asia Pacific. • The threat actor left a ransom note claiming that data was extracted from the Organization's systems, and also threatened to publish data. • The Organization received evidence that data from servers located in the UK and Australia was extracted. Systems in Canada remain unaffected and secure. • The incident did not affect the Organization's Canadian HR system, but it may have affected personal information relating to the company shareholdings of one employee who resides in Alberta.
Affected individuals	The incident may have affected one (1) individual whose personal information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Offered the affected individual 12 months of identity theft and credit monitoring. • Disconnected affected systems from the network. • Reset administrator passwords and implemented a forced password reset for all users. • Added other security measures. • Engaged external cyber security specialists to investigate. • Notified privacy regulators outside of Canada and law enforcement in the UK. • Working with a third-party cybersecurity firm to investigate the root cause of the incident and will undertake a detailed review of its cyber security policies and procedures to implement further enhancements to its security posture.
Steps taken to notify individuals of the incident	The affected individual in Alberta was notified in writing on April 14, 2021
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, *… whilst there is evidence of data having been extracted from …systems in the UK and Australia, there is no evidence of data concerning the affected individual having been affected. In the event of exfiltration, personal information about the affected individual could potentially trigger a risk of fraud.* In my view, a reasonable person would consider that the contact and financial information at issue could be used to cause the significant harms of identity theft or 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 its belief…. *… that the motive behind the threat actor's actions is to extort a ransom payment … rather than to exploit and misuse personal information. As such, [the Organization] assesses the risk to the affected individual to be low.* In my view, a reasonable person would consider 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, ransom demand). The Organization can only speculate as to the motives of the perpetrator.

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 individual.

A reasonable person would consider that the contact and financial information at issue could be used to cause the significant harms of identity theft or fraud. 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, ransom demand). The Organization can only speculate as to the motives of the perpetrator.

I require the Organization to notify the affected individual 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 in writing on April 14, 2021. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner