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	Acquis Consulting Group, LLC (Organization)
Decision number (file number)	P2019-ND-053 (File #011254)
Date notice received by OIPC	December 20, 2018
Date Organization last provided information	December 20, 2018
Date of decision	May 3, 2019
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 a management consulting firm based in the United States with a limited number of employees in foreign jurisdictions. 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 some or all of the following types of information: • name, • date of birth, • passport number, • email address, • home address, • social security number, • alien registration number, • taxpayer identification number, and • health insurance information (subscriber, policy, and group numbers). This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent this information was collected in Alberta, PIPA applies in this matter.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On November 12, 2018, the Organization discovered a potential security incident. • An investigation found that an employee email account had been accessed by an unauthorized actor. The Organization reported the incident occurred between "June 30-June 2, 2018 [sic]". • On November 12, 2018, the Organization learned that certain personal information was contained in the email account. • On December 8, 2018, the Organization found that the personal information of Albertans was potentially involved.
Affected individuals	The breach affected 2 individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Investigated and engaged a cybersecurity and forensic firm. • Confirmed that IT systems are secure and not infected by malware or any other malicious program. • Quarantined affected email and changed login credentials. • Offering affected individuals free dark web monitoring services at no cost for two years. • Reviewing security measures, internal controls, and safeguards and continuing to make changes to help prevent a similar incident from occurring in the future. • Engaged a vendor to provide anti-phishing testing and training to employees. • Notified applicable data protection authorities.
Steps taken to notify individuals of the incident	The Organization reported that "All affected individuals will be sent written notification of the incident on December 21 2018".
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 "…the unauthorized access to the personal information of affected individuals (assuming the unauthorized access occurred) could potentially be used to conduct identity theft and/or fraud". I agree with the Organization's assessment. A reasonable person would consider that the contact, identity and health information at issue could be used to cause the significant harms of identity theft and fraud. Email address could be used for phishing purposes, increasing vulnerability to the 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 that "The likelihood that harm may occur to any of the affected individuals is moderate. The Incident involved the malicious intent on the part of an unknown third party. However, the forensic evidence obtained from the investigation additionally suggests that the third party was actually attempting to determine a way to fraudulently divert funds from [the Organization] rather than targeting and/or stealing the personal information/credentials of individuals. Additionally, the Incident occurred in June of 2018 and to date [the Organization] has no evidence that any of the affected individuals have been subject to identity theft and/or fraud". In my view, a reasonable person would consider that the likelihood of harm resulting in this case is increased because the breach resulted from malicious intent (deliberate action by unknown and unauthorized third party). The Organization can only speculate on the motives of the unknown third party, but, even so, believes the motive to be fraudulent. The fact the Organization has not been made aware of actual identity theft and/or fraud does not preclude such harms from occurring in the future.

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 contact, identity and health information at issue could be used to cause the significant harms of identity theft and fraud. Email address could be used for phishing purposes, increasing vulnerability to the harms of identity theft and fraud. The likelihood of harm resulting in this case is increased because the breach resulted from malicious intent (deliberate action by unknown and unauthorized third party). The Organization can only speculate on the motives of the unknown third party, but, even so, believes the motive to be fraudulent. The fact the Organization has not been made aware of actual identity theft and/or fraud does not preclude such harms from occurring in the future.

I require the Organization to notify the affected individuals whose personal information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the affected individuals were notified of the breach on December 21, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner