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	Martin Energy Group Services, LLC (Organization)
Decision number (file number)	P2022-ND-038 (File #022869)
Date notice received by OIPC	August 20, 2021
Date Organization last provided information	August 20, 2021
Date of decision	May 18, 2022
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify the 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 a solutions provider for generator packages, combined heat and power systems, microgrids, landfill gas, wastewater treatment anaerobic digester design and construction. It is headquartered in Missouri, United States, has an office in Ontario and operates in Alberta. The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The Organization reported a phishing event and business email compromise involved some or all of the following employee and subcontractor information: • social insurance numbers, • bank names, • financial account numbers, • dates of birth, • debit and credit card numbers, • drivers' licenses, • other government IDs and employee IDs. 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 January 25, 2021, the Organization discovered that it had been subject a phishing event and business email compromise. • The Organization identified the specific mailboxes subject to suspicious activity. It reported there was no indication that the mailboxes were taken offline or exfiltrated, only that rules were created within the mailboxes for internal transfer and not a transfer to an external email address. • The Organization forensics team have been unable to confirm or rule out specific access to individual emails and therefore treated the entirety of the mailboxes as accessed by the unknown third-party actor. • The Organization's investigation was able to establish that the period of unauthorized access spanned from January 19, 2021 to February 3, 2021.
Affected individuals	The incident affected approximately 466 individuals, including 2 individuals whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Secured the affected accounts immediately. • Changed all the passwords on its employees' email accounts. • Hired experts to conduct a forensic investigation. • Hired experts to undertake a data mining exercise to identify the specific email accounts affected by the incident and the personal information that could have been potentially accessed by the unknown threat actors. • Offered a complimentary 12-month subscription to credit monitoring services.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on August 23, 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, *The possible consequences might include the loss of confidentiality of personal data, increased exposure to phishing attacks, identity theft, and fraudulent transactions.* In my view, a reasonable person would consider that the contact, identity, employment and financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. The Organization recognized that information at issue could be

	used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all 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 possible harm.	The Organization reported, *Martin Energy has no indication that any personal information has been subject to actual or attempted misuse in relation to this Incident.* In my view, a reasonable person would consider that 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 into an employees' email account). The Organization reported that it "*has no indication that any personal information has been subject to actual or attempted misuse in relation to this incident*." The lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing, identity theft and fraud can occur months and even years after a data breach. The Organization also reported that the "*forensics team have been unable to confirm or rule out specific access to individual emails and have therefore treated the entirety of the mailboxes as accessed by the unknown third-party actor."* Further, the information may have been exposed for approximately 3 weeks.

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, employment and financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. The information at issue could be used for the purposes of phishing, increasing the affected individuals' vulnerability to identity theft and fraud. These are all significant harms.

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 into an employees' email account). The lack of reported incidents resulting from this breach to date is not a mitigating factor, as phishing, identity theft and fraud can occur months and even years after a data breach. The Organization also reported that the "*forensics team have been unable to confirm or rule out specific access to individual emails and have therefore treated the entirety of the mailboxes as accessed by the unknown third-party actor*." Further, the information may have been exposed for approximately 3 weeks.

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 Organization notified affected individuals by letter on August 23, 2021, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Cara-Lynn Stelmack
Assistant Commissioner, Operations and Compliance