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	Matrix Service Company (Organization)
Decision number (file number)	P2016-ND-36 (File #002872)
Date notice received by OIPC	March 11, 2016
Date Organization last provided information	May 18, 2016
Date of decision	July 8, 2016
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 headquartered in Tulsa, Oklahoma and operates throughout the United States and Canada, including in Alberta. The Organization is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, • employee identification number, • social insurance number, • social security number, • salary information. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. Some of the information was collected in Alberta.

DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ☒ unauthorized disclosure	
Description of incident	• On February 3, 2016, an employee of the Organization received a phishing email, disguised as an email from the Organization's CEO. The email requested names, addresses, social security numbers, social insurance numbers, dates of birth, and salary information for all active employees, including those of the Organization's subsidiary companies. • Believing the email to be legitimate, the employee replied to the message on the day the email was received and attached a spreadsheet with the requested data. • The Organization learned of the incident on February 29, 2016, through the employee who had responded to the phishing email.
Affected individuals	A total of 4,651 individuals were affected, 585 of whom are Canadian residents, and 35 of whom are residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Immediately launched an internal investigation of the matter. • Contacted the United States Federal Bureau of Investigations and Internal Revenue Service as well as Canada Revenue Agency. • Offered the affected individuals two years of credit monitoring and identity theft protection through Equifax Canada, at no cost to the individuals. • Provided affected individuals with information about activating monitoring and /or additional protections available from Canada Revenue Agency, Service Canada, and consumer protection agencies. • Provided a call center support for the affected individuals to respond to questions or concerns about the incident. • Reinforcing information security training to emphasize the detection and avoidance of phishing email scams and identifying opportunities to increase security within information technology systems.
Steps taken to notify individuals of the incident	• On March 3, 2016, an email notification of the incident was sent to all current employees. • On March 11, 2016, written notice of the incident was sent to the home addresses of the affected current and former employees.

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 "Identity theft or negative effects on a credit record may result from the incident", noting that "The information on the spreadsheet included SINs". I agree with the Organization. The personal information at issue includes sensitive identity information that could be used to cause the harms of identity theft and fraud or financial loss. 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 possible harm.	In its report, the Organization did not assess the likelihood of harm resulting from this incident, but said that "Identity theft or negative effects on a credit record may result…". In my view, the likelihood of harm resulting from this incident is increased because the incident resulted from deliberate action (perpetrator impersonated a senior member of the Organization), indicating malicious intent, and the circumstances suggest the information at issue was the target.

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. The personal information involved is sensitive identity information that could be used to cause the harms of identity theft and fraud or financial loss. The incident resulted from deliberate action (perpetrator impersonated a senior member of the Organization), indicating malicious intent, and the circumstances suggest the information at issue was the target.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individuals on March 11, 2016 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner