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	Midwest Surveys Inc. (Organization)
Decision number (file number)	P2020-ND-070 (File # 015699)
Date notice received by OIPC	April 22, 2020
Date Organization last provided information	April 22, 2020
Date of decision	July 15, 2020
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 information at issue includes: • name, • salary, • tax information(T4/TS/TS008), • position, • personal email address, • client email address, • healthcare number, • social insurance number, • bank dealt with, • online trading account information, • online gambling account information. 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 April 3, 2020 a series of emails, with a link to virus payload, was sent out from an employee's email account. • The Organization reported the "… account had been compromised by a bad actor at some point, but there was no evidience [sic] other than the series of emails with a malicous [sic] link being sent on their behalf. User could not recall any of the possible situations described to them by the investigator that may have led to giving out their email and password." • The breach was reported the same day by a number of employees who received suspicious emails.
Affected individuals	The Organization reported the incident affected 1 individual.
Steps taken to reduce risk of harm to individuals	• Locked out the affected user's account and notified the rest of the company not to open emails from that account. • Deleted all emails that were sent out from the Organization's system and notified all clients that received an email from the compromised account. • Scanned computer for additional malware or viruses. • Changed account passwords and email address. • Reviewed policy regarding sending passwords in emails. • Will continue to educate users about email phishing and how to avoid computers and accounts from being compromised. All company email accounts to be set up with multi-factor authentication.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on April 3, 2020.
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 "Identity theft could occur using the healthcare/SIN/tax/salary/bank information (no banking passwords found) that was present in the email account." In my view, a reasonable person would consider the contact, identity, financial, health, employment and tax information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing, increasing vulnerability to 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	The Organization reported: *Based on the likelihood of significant harm, I'd have to assess this breach in the high risk category. There's evidence of malicious intent but no relationship exists with unintended recipient. Internal/external email addresses*

between the incident and the possible harm.	*were exposed. However, there was individually identifying information (i.e. SIN, banking info, date of birth, health info, etc.) in the acccount [sic] as a source for possible identity theft.* 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. The compromised email account was used to send phishing emails.
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 the contact, identity, financial, health, employment and tax information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing, increasing vulnerability to identity theft and 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. The compromised email account was used to send phishing emails. 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 affected individuals were notified by email on April 3, 2020. The Organization is not required to notify the affected individuals again.	

Jill Clayton
Information and Privacy Commissioner