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)	P2019-ND-068 (File #011948)
Date notice received by OIPC	February 4, 2019
Date Organization last provided information	February 4, 2019
Date of decision	June 27, 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 operates in Alberta and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	Depending on the extent of the access, the incident may have involved some or all of the following types of information: • name, • salary, • position, • personal email address, • client email address, • corporate credit card information. With the exception of corporate credit card 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 or about January 15, 2019 a staff member's personal Gmail account was phished. • The Organization reported the account "…likely contained [the employee's] work password, they planted a pdf on the individual's work OneDrive that they then shared out to some clients and employees in the address book. The second, third and fourth person opened the shared file and entered their user and password, their account was considered compromised at that point". • The Organization reported the phishing email originated from inside the company. • The incident was discovered on January 21, 2019.
Affected individuals	The incident affected 4 individuals.
Steps taken to reduce risk of harm to individuals	• Locked out affected user accounts within half an hour and notified employees not to open emails from certain identified individuals. • Deleted all emails that were sent out, checked for emails that were sent to clients from affected accounts. • Scanned computers for individuals whose accounts were compromised for any additional malware or viruses. Changed account passwords. Advised individuals to go through in boxes and notify personal and client contacts of the breach. They were advised to change all account passwords for personal emails, banks and subscription services. • Cancelled corporate credit card. • Installed a threat protection service on all email accounts. • Revisited policy regarding sending passwords in emails was revisited. Will continue to educate users about email phishing and how to avoid computers and accounts being compromised.
Steps taken to notify individuals of the incident	Affected individuals were notified on January 21, 2019 by telephone and in person, and by email.
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 "Salary information could be used for embarrassment or humiliation. The names of individuals in the company and client address books could be used for further phishing attacks. Corporate credit card data could be used for identity theft". I agree with the Organization. A reasonable person would consider that contact and employment information, particularly with email address, could be used for phishing, increasing vulnerability to identity theft and fraud. Salary information could be used to cause embarrassment or humiliation. 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.	The Organization reported that "Based on the likelihood of significant harm, I'd have to assess this breach in the moderate category. There's evidence of malicious intent, no relationship exists with unintended recipient, credit card enable the breach as a single source for identity theft information was present, and internal/external email addresses were exposed. However, there was no personal identity information (i.e. SIN, banking info, date of birth, health info, etc.) to enable the breach as a single source for identity theft." In my view, a reasonable person would consider that the likelihood of phishing harm resulting in this case is increased because the breach resulted from malicious intent. The perpetrator is not known, however, so it is unclear if there are personal/professional relationships that would make embarrassment/humiliation more likely.

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 contact and employment information, particularly with email address, could be used for phishing, increasing vulnerability to identity theft and fraud. Salary information could be used to cause embarrassment or humiliation. These are significant harms.

The likelihood of phishing harm resulting in this case is increased because the breach resulted from malicious intent. The perpetrator is not known, however, so it is unclear if there are personal/professional relationships that would make embarrassment/humiliation more likely.

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 on January 21, 2019 by telephone and in person, and by email. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner