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	Midnight Integrated Financial, Inc. (Organization)
Decision number (file number)	P2019-ND-160 (File #013058)
Date notice received by OIPC	April 23, 2019
Date Organization last provided information	September 11, 2019
Date of decision	October 24, 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 an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • salary, and • photograph (for one individual), • employee email address, • personal information potentially contained in staff emails. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• In early February 2019, an employee's email account was compromised as a result of a phishing email.

	• On March 1, 2019, the Organization's external IT service provider emailed administration credentials to the employee that were then used by the unauthorized user on March 5, 2019 to delegate the inboxes of six (6) additional staff to the employee. • The employee identified the issue and reported it to the Organization's IT personnel. The inbox delegations were removed and all passwords reset. • The Organization's investigated and found that 35 documents were viewed by the unauthorized party. The investigation also found there was no indication of persistent compromise and it is not believed that the attack resulted in the installation of malware. • The forensics analysis was not able to confirm or rule out access to or exfiltration of information in emails but due to the pattern of the attack, the likelihood was deemed to be low.
Affected individuals	The incident affected 12 individuals residing in Alberta.
Steps taken to reduce risk of harm to individuals	• Disabled inbox delegation. • Notified all employee users. • Required a change in password and enabled two-factor authentication for administrator accounts. • Conducted an investigation. • Engaged a cyber security consultant. • Hired an IT forensic firm to investigate the incident and enhance existing security safeguards. • Ongoing meetings of the management regarding cybersecurity. • Additional training for employees.
Steps taken to notify individuals of the incident	The Organization reported that "All …employees were immediately notified of the incident, verbally and/or via email, during the containment efforts after [the Organization] was alerted of the incident on March 5, 2019."
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 "Forensic analysis could not definitively confirm this was the case but there were several indicators in the pattern of compromise that would suggest the perpetrators were specifically motivated, specifically targeting credit card and bank account-related information. None of the accessed Documents contained such information…". The Organization reported that it…

	… conducted an assessment of the Email information and came to the conclusion that it was unlikely that delegated staff inboxes would contain any sensitive personal identifiers of any third parties such as SINs, credit card numbers, driver's license, passport, or account numbers. In my view, a reasonable person would consider the contact (name) and financial information (salary) at issue could be used to cause the harms of hurt, humiliation and embarrassment. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are all significant harms. Because the Organization cannot identify whether other personal information in the employee emails was accessed, it is not clear what other possible harms may exist.
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 risk of harm based on the compromise of the Accessed Documents was low – the sensitivity of the data was deemed low, and the information likely targeted by the attackers was not contained in the Access Documents…* *[The Organization] is not aware of any suspicious activity or any indication of misuse or harm to individuals noted since the incident. Based on this assessment (the Organization) made the determination that there was not a real risk of significant harm to any individual as a result of potential access to Email information.* The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (phishing) by an unknown third party and it appears the personal information may have been used to send fraudulent emails, with the purpose of obtaining information for fraudulent purposes. The Organization cannot rule out the possibility that unauthorized persons accessed, read, copied, or downloaded personal information within the documents or employee emails. The lack of reported incidents to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. Further, the information may have been exposed for approximately one (1) month.
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 (name) and financial information (salary) at issue could be used to cause the harms of hurt, humiliation and embarrassment. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. These are all significant harms. Because	

the Organization cannot identify whether other personal information in the employee emails was accessed, it is not clear what other possible harms may exist.

The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (phishing) by an unknown third party and it appears the personal information may have been used to send fraudulent emails, with the purpose of obtaining information for fraudulent purposes. The Organization cannot rule out the possibility that unauthorized persons accessed, read, copied, or downloaded personal information within the documents or employee emails. The lack of reported incidents to date is not a mitigating factor, as identity theft and fraud can occur months and even years after a data breach. Further, the information may have been exposed for approximately one (1) month.

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

I understand the Organization notified its employees verbally and in an email dated March 5, 2019 in accordance with the Regulation. The Organization is not required to notify these affected individuals again.

The Organization is required to confirm to my Office in writing, within ten (10) days of the date of this decision, that it has reviewed the employee emails at issue to identify any additional affected individuals, and, if there are additional affected individuals, that these individuals have been notified of this incident in accordance with the requirements outlined in the Regulation.

Jill Clayton
Information and Privacy Commissioner