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	AccSys, LLC d/b/a/ Restaurant Magic (Organization)
Decision number (file number)	P2020-ND-181 (File #015770)
Date notice received by OIPC	May 8, 2020
Date Organization last provided information	May 8, 2020
Date of decision	December 8, 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 the individual 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 incident involved the following information: • name, • address, and • digital signature. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• Around March 10, 2020, the Organization was alerted to suspicious activity within four (4) email accounts belonging to email users of the Organization.

	• The Organization determined that email accounts were accessed without authorization between March 4, 2020 and March 10, 2020; only one (1) of the email accounts was accessed for the entire time.
Affected individuals	The incident affected 159 individuals, including one (1) individual in Alberta.
Steps taken to reduce risk of harm to individuals	• Investigated and responded to the incident. • Assessed the security of its systems. • Implemented additional safeguards, including mandatory training for all email users and presentations regarding social engineering, phishing etc., enhanced logging with notifications, multi-factor authentication for all users and implementing stricter email protocols. • Provided access to identity monitoring services for 24 months to affected individuals at no cost. • Provided resources to potentially affected individuals, e.g. how to better protect against identity theft or fraud to their credit card company/bank, how to place a fraud alert and security freeze one's credit file, information about protecting from tax fraud, a reminder to remain vigilant, etc. • Notified certain regulators as required.
Steps taken to notify individuals of the incident	Affected individual was notified by letter on May 8, 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 did not specifically identify the type of harm(s) that might result from this incident but reported it "...is providing potentially impacted individuals with resources ...including guidance on how to better protect against identity theft and fraud". Given the above, I believe a reasonable person would consider that the personal information at issue could be used to cause the significant harms of 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 between the incident and the possible harm.	The Organization did not specifically address the likelihood of significant harm resulting from this incident; however, the Organization took several steps to enhance its privacy and security safeguards and offered credit monitoring services to the affected individual. The Organization also reported "At this time, we are unaware of any actual or attempted misuse of personal information relating to this event."

	In my view, a reasonable person would consider that the likelihood of significant harm resulting from this incident is increased as it resulted from deliberate, unauthorized action. The email accounts were exposed over the course of 6 days.

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 personal information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of significant harm is increased as the incident resulted from deliberate, unauthorized action. The email accounts were exposed over the course of 6 days.

The Organization is required to notify the affected individual whose personal information was collected in Alberta, pursuant to section 37.1 of PIPA. I understand the affected individual was notified by letter on May 8, 2020. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner