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	Master-Bilt Refrigeration Solutions (Organization)
Decision number (file number)	P2020-ND-050 (File #014047)
Date notice received by OIPC	December 3, 2019
Date Organization last provided information	December 3, 2019
Date of decision	May 21, 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 of an Alberta resident: • name, and • payment card number including expiry date and security code. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• The Organization learned that a number of spam emails had been sent from an employee's account. • An investigation determined that an unauthorized person accessed the account between July 10-11, 2019. The investigation was unable to determine which specific emails or attachments, if any, were viewed by the unauthorized individual.

	• On November 7, 2019, the Organization determined that the unauthorized individual accessed the personal information of one Alberta resident.
Affected individuals	The incident affected one individual residing in Alberta
Steps taken to reduce risk of harm to individuals	• Investigated and retained a cybersecurity firm to assist. • Reminded affected individuals to review account statements and report any unauthorized charges to financial institutions. • Implemented additional safeguards and technical security measures to help prevent a similar occurrence in the future.
Steps taken to notify individuals of the incident	Affected individuals were notified by mail on December 2, 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 "Stolen payment card information can be used to make fraudulent purchases on the impacted card". In my view, a reasonable person would consider that the financial information at issue could be used to cause the harms of identity theft and fraud. 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 "The payment card network rules generally provide that cardholders are not responsible for unauthorized charges that are timely reported. [The Organization] is providing notice to the individuals involved as soon as reasonably possible so that they can remain vigilant to potential unauthorized charges. Therefore, there is not a substantial likelihood that the individuals involved will experience financial harm as a result". In my view, a reasonable person would consider 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 (deliberate intrusion). The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

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 individual. A reasonable person would consider that the financial information at issue could be used to cause the harms of identity theft and fraud. These are significant harms. 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 (deliberate intrusion). The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud. I require the Organization to notify the affected individual whose information was collected in Alberta, in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified affected individuals by letter on December 2, 2019 in accordance with the Regulation. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner