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	WESCO Distribution Inc. (Organization)
Decision number (file number)	P2020-ND-065 (File#015224)
Date notice received by OIPC	February 27, 2020
Date Organization last provided information	February 27, 2020
Date of decision	July 13, 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 incident involved all or some of the following information for 4 individuals: • name, • street address, • telephone number, • email address, • date of birth, and • financial information (bank account number, routing number, financial institution name) for one affected individual. 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	• On July 1, 2019, the Organization learned an employee's email account was compromised by an unknown actor through a phishing email sent on August 15, 2018 from a well-known supplier of the Organization. • The attack spread to 28 other user accounts. • The unknown actor placed an automatic forwarding rule on the accounts, which forwarded all incoming emails to an unauthorized Gmail account. • The Organization disabled the rule on July 1, 2019 and reported there was no further unauthorized disclosure of personal information in connection with this incident.
Affected individuals	A total of 769 individuals were affected, including 306 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Disabled the auto-forward rule upon discovering the issue. • Offered one-year enrollment in a plan that includes credit monitoring, internet and dark web scanning, limited identity theft insurance, assistance protecting against theft of personal information and access to a customer care representative. • Launched an internal investigation and amended its administrative and technical safeguards. • Changed the access credentials for the impacted accounts. • Enabled Microsoft's 'conditional access" to its email system, and is implementing multi-factor authentication to ensure greater security.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on February 20, 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: *Of the Alberta residents impacted by the breach, the potential harm(s) vary depending upon the type of information impacted for each individual. Individuals whose email addresses and/or dates of birth were impacted may be at risk of phishing. The Alberta resident whose financial information was impacted may be at risk of financial harms such as theft or fraud…we believe such risk to be low.* In my view, a reasonable person would consider the contact, identity and financial information at issue could be used to cause the significant harms of identity theft, fraud, and financial loss. Email address 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 between the incident and the possible harm.	The Organization reported that, *Based on the nature of the incident, we believe the most significant risk to the Alberta residents would be phishing attempts directed at the impacted parties. Further, while there were a large number of emails involved in the incident, only a small subset contained personal information. None of the information involved in the incident would, by itself, allow access to a financial account. For those reasons, we believe the risk to the Alberta residents of theft or fraud is low.* 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 (phishing). 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 the unauthorized party viewed, read, copied, or downloaded the affected individual's personal information. Further, the personal information may have been exposed for approximately 11 months.

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 and financial information at issue could be used to cause the significant harms of identity theft, fraud, and financial loss. Email address could be used for phishing, increasing vulnerability to identity theft and fraud. 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 (phishing). 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 the unauthorized party viewed, read, copied, or downloaded the affected individual's personal information. Further, the personal information may have been exposed for approximately 11 months.

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 the Organization notified affected individuals by letter on February 20, 2020. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner