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	AltaSteel, Inc. (Organization)
Decision number (file number)	P2021-ND-003 (File #018358)
Date notice received by OIPC	November 23, 2020
Date Organization last provided information	November 27, 2020
Date of decision	January 26, 2021
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. The Organization is required to notify 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: • name, • address, • social insurance number, and • date of birth. 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 November 18, 2020, two employees reported receiving bounce back emails indicating "Your organization does not allow external forwarding". • The Organization investigated, and on November 20, 2020, confirmed that 5 employee email accounts were set up with rules forwarding emails to an external email address. Of these 5, three (3) did not appear to be set up by individuals and were

	forwarded to external unknown email addresses (@gmail.com). • The Organization reported the forwarding rules were set up on or about August 21, 2020.
Affected individuals	The incident affected 400 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Shut down the email forwarding and made changes to the global email system to not allow forwarding outside the Organization. • Reviewing option to offer credit monitoring services for affected employees.
Steps taken to notify individuals of the incident	The Organization reported affected individuals were "Not currently notified will be notified by the end of the week".
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 the possible harm that might result from this incident is "identity theft". I agree with the Organization's assessment. A reasonable person would consider that the contact and identity 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 reported "Likelihood not sure at this time [sic], risk could be significant if identity theft did occur." 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 (deliberate intrusion and forwarding of personal information). Further, the information may have been exposed for approximately three 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 that the contact and identity information at issue could be used to cause the significant harms of identity theft and fraud. 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 and forwarding of personal information). Further, the information may have been exposed for approximately three 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), and confirm to my Office, within ten (10) days of the date of this decision, that this has been done.

Jill Clayton
Information and Privacy Commissioner