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	Woodstream Canada (Organization)
Decision number (file number)	P2021-ND-266 (File #020237)
Date notice received by OIPC	March 23, 2021
Date Organization last provided information	March 23, 2021
Date of decision	February 9, 2022
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 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 the following information: • name, • telephone number, • email and residential address, and • order details. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the information at issue was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On August 24, 2020, the Organization discovered that a third party gained unauthorized access to the e-commerce platform of DynaTrap, a subsidiary of the Organization. • A vulnerability on the e-commerce platform allowed for unauthorized installation of code on compromised systems.

	• Data sent to and from the e-commerce platform between August 24, 2020, until September 9, 2020 may have been intercepted. • On September 9, 2020, the access was terminated. • The Organization investigated and identified the potentially compromised data with assistance from its IT experts. While there was no positive evidence of data exfiltration, the possibility could not be ruled out given that the attackers had access to the systems.
Affected individuals	The incident affected 1,883 individuals, including 246 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Brought the site offline until investigation and recovery efforts could take place. • Recommended steps to affected individuals to protect themselves from potential misuse of their personal information. • Took steps to resolve the vulnerability. • Shut down the website on the e-commerce platform in question and transitioned it to a different platform that does not have the vulnerability.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on March 17, 2021
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, *While the organization assesses the risk of harm as low, affected individuals may be subject to phishing attempts or unsolicited communications.* I agree with the Organization. A reasonable person would consider that the contact information, including email address, particularly in association with order information, could be used for the purposes of phishing, increasing the affected individuals' vulnerability to 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	The Organization reported, *Risk of harm is assessed as low. There is no evidence of exfiltration or actual unauthorized access.* In its notice to affected individuals, the Organization stated:

between the incident and the possible harm.	*We encourage you to remain vigilant against incident of fraud or identity theft, from any source, and to monitor your accounts and credit reports, generally, for suspicious activity and to detect any errors. You may also review the enclosed Steps You Can Take to Protect Personal Information for additional guidance on how to protect against actual or attempted fraud or misuse.* 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). Although the Organization said there is no evidence of exfiltration or actual unauthorized access, the Organization also said it "could not be ruled out given that the attackers had access to the systems." The lack of reported incidents of identity theft or fraud to date is not a mitigating factor, as identity theft can happen months and even years after a data breach. Further, the information may have been exposed for approximately two weeks.

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 information, including email address, particularly in association with order information, could be used for the purposes of phishing, increasing the affected individuals' vulnerability to 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). Although the Organization said there is no evidence of exfiltration or actual unauthorized access, the Organization also said it "could not be ruled out given that the attackers had access to the systems." The lack of reported incidents of identity theft or fraud to date is not a mitigating factor, as identity theft can happen months and even years after a data breach. Further, the information may have been exposed for approximately two weeks.

I require the Organization to notify the affected individuals 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 March 17, 2021 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner