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	The Debriefing Academy Inc. (Organization)
Decision number (file number)	P2021-ND-241 (File #018777)
Date notice received by OIPC	December 17, 2020
Date Organization last provided information	July 28, 2021
Date of decision	November 30, 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 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 operates in Alberta and 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, • email address, • mailing address, • telephone number, • work affiliation, and • professional background. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization uses a third party (Webeteer Inc.) for website development and support. At the time of the breach, Webeteer Inc. subcontracted hosting to another third party, GreenGeeks. • On December 6, 2020, the Organization found that its WordPress website was not functioning properly. The Organization notified its website development provider who subsequently responded to the incident. • The Organization determined that a malicious actor gained access to the server environment, which includes a database of registered clients, by exploiting a vulnerable WordPress plugin. • It also reported that the attacker(s) installed malware, and created new email and file-transfer protocol (FTP) accounts. • Attempts to access the environment without authorization were detected for a number of days after the breach was contained. • The Organization reported the breach occurred between December 6-8, 2020.
Affected individuals	The incident affected 140 individuals, including 8 whose information was collected in Alberta.
Steps taken to reduce risk of harm to individuals	• Suspended the server. • Removed database of registered users from website. • Ran diagnostics and malware scans. • Sanitized the server, including removal of malware and unused plugins. • Changed all passwords. • Deleted email and FTP accounts created by the attacker(s). • Migrated services to a new hosting provider. • Implemented a "maintenance plan" that includes updating plugins and core WordPress components. • Setup two-factor security.
Steps taken to notify individuals of the incident	Affected individuals were notified by email on December 9, 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	The Organization reported: *… it is possible that some of this information could be used to initiate some level of identity theft, such as e-mails being used to initiate phishing attempts.* I agree with the Organization's assessment. A reasonable person would consider that professional information and email addresses,

non-trivial consequences or effects.	in conjunction with knowledge that the affected individuals are customers of the Organization, 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 between the incident and the possible harm.	The Organization reported: *We do not believe that access to this personal information represents a real risk of significant harm to them, as the personal information collected does not include sensitive information (such as health information, financial information, Social Insurance Numbers / Social Security Numbers).* In my view, the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of a third party (deliberate intrusion and installation of malware). Further, after containing the breach, the Organization detected ongoing attempts to access the environment without authorization, suggesting that the server was being actively exploited.

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 professional information and email addresses, in conjunction with knowledge that the affected individuals are customers of the Organization, 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 a third party (deliberate intrusion and installation of malware). Further, after containing the breach, the Organization detected ongoing attempts to access the environment without authorization, suggesting that the server was being actively exploited.

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 email on December 9, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner