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	Vitalize, LLC (Organization)
Decision number (file number)	P2019-ND-193 (File #013295)
Date notice received by OIPC	May 15, 2019
Date Organization last provided information	May 15, 2019
Date of decision	December 13, 2019
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 information at issue included: • name, • email address, • Bodybuilding.com password, • billing/shipping address, • telephone number, • order history, • any communications with Bodybuilding.com, • date of birth, • any information a customer included in their BodySpace profile (note: profile information is generally already publicly visible to others). 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	• In February 2019, the Organization became aware of a data security incident involving unauthorized access to its systems. • The Organization's investigation traced the unauthorized activity to a phishing email received in July 2018. • The investigation also determined that some data was removed from the Organization's systems, but the nature of the files taken is unknown.
Affected individuals	The incident affected approximately 45,615 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Re-setting all customer passwords. • Took steps to secure networks and assess the incident with outside counsel and a leading forensic security firm. • Monitoring account activity and the dark-web. • Will work with security experts to enhance systems to detect and prevent unauthorised access to personal data. • Implemented additional email and internal-system security measures and will continue to provide regular reminders and training for employees and representatives on how to spot and avoid being victimized by phishing emails in the future. • Working with security experts to determine appropriate additions or changes if any, to its security software suite.
Steps taken to notify individuals of the incident	Affected individuals were notified by email April 30, 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 it… *…has no information indicating the extent of personal data that was compromised, and does not have any information that personal data has been misused. The identity and motive of the attacker remain under investigation. We are still assessing the potential consequences of the incident.* *We have no information at this time that the attacker accessed or exfiltrated any customer personal data. However, if a malicious actor did access customer personal data, with sufficient technical skills and resources, it may be possible for such an actor to leverage some of those passwords for account access to other websites. Because such an outcome would depend on the sophistication and determination of the bad actor and other factors, we cannot comment on the likelihood of this occurring.* In my view, a reasonable person would consider that the contact, identity and profile information at issue could be used to cause the

	harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Credentials (password) could be used to compromise other online accounts. These are all 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.	As noted above, the Organization reported that "Because such an outcome would depend on the sophistication and determination of the bad actor and other factors, we cannot comment on the likelihood of this occurring." In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (phishing email) and "some data was removed from the Organization's systems". The breach was not discovered for 7 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, identity and profile information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. Credentials (password) could be used to compromise other online accounts. These are all significant harms.

The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (phishing email) and "some data was removed from the Organization's systems". The breach was not discovered for 7 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 affected individuals were notified by email April 30, 2019. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner