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	Grass Advantage, LLC d/b/a Amazing Grass (Organization)
Decision number (file number)	P2017-ND-163 (File #007298)
Date notice received by OIPC	December 6, 2017
Date Organization last provided information	December 6, 2017
Date of decision	December 11, 2017
Summary of decision	There is a real risk of significant harm as a result of this incident. The Organization is required to notify the affected individual 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, • contact information, • credit card number, expiry date and card verification number. This information is about an identifiable individual and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected from customers making purchases via the Organization's website, www.AmazingGrass.com.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On November 3, 2017, the Organization was alerted to a potential security incident affecting its website and online store at www.AmazingGrass.com. • The Organization engaged an independent forensic firm to assist in its investigation of this matter.

	• Based on the investigation, the Organization believes that malicious software designed to capture payment card data was installed by an unauthorized individual on portions of the website. • Information entered by certain customers when making purchases on the website between September 11, 2017 and November 3, 2017 may have been affected.
Affected individuals	The incident may have affected one (1) resident of Alberta.
Steps taken to reduce risk of harm to individuals	• Initiated an investigation and took steps to ensure that the malicious software was removed from the website and that the incident had been contained. • Continuing to work with the company that hosts and manages the website to make additional updates and enhancements to security. • Notified law enforcement.
Steps taken to notify individuals of the incident	The one (1) Alberta resident who may have been affected by the incident was notified via written email on or about December 1, 2017 and offered 12 months complimentary identity monitoring services.
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 "In some cases incidents that affect credit card numbers could potentially result in attempted or fraudulent transactions involving that card." In my view, the financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. 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 that "Out of an abundance of caution, [the Organization] is notifying the potentially affected Alberta customer about this incident and providing information and resources to help this individual protect themself." In my view, the likelihood of harm is increased because the incident resulted from malicious intent (deliberate intrusion and malware), and the information was exposed (collected) over a period of almost two 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 as a result of this incident. The financial information at issue could be used to cause the harms of identity theft, fraud and financial loss. The likelihood of harm is increased because the incident resulted from malicious intent (deliberate intrusion and malware), and the information was exposed (collected) over a period of almost two months. The Organization is required to notify the affected individual in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand the Organization notified the affected individual by written email on or about December 1, 2017. The Organization is not required to notify the affected individual again.

Jill Clayton
Information and Privacy Commissioner