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	GS1 US, Inc. (Organization)
Decision number (file number)	P2019-ND-125 (File #010452)
Date notice received by OIPC	November 6, 2018
Date Organization last provided information	November 6, 2018
Date of decision	August 2, 2019
Summary of decision	There is a real risk of significant harm to the individuals affected by this incident. Pursuant to section 37.1 of the *Personal Information Protection Act* (PIPA), the Organization is required to notify those individuals whose personal information was collected in Alberta.
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 Organization reported "The personal information that was involved in the incident may have included first and last name, company name, address, phone number, email address, and payment card information including account number, expiration date, and three-digit security code." The Organization also said "We want to stress that these customers are business entitles and not individuals, but we have decided to notify them out of an abundance of caution in the event that any personal information may have been associated with the online transactions." Given the above, it appears that most, if not all, of the personal information at issue may qualify as "business contact information" which is defined in section 1(1)(a) of PIPA to mean "an individual's name, position name or title, business telephone number, business address, business email address, business fax number and other similar business information." Section 4(1)(d) of PIPA says that the Act does not apply to the collection, use and disclosure of business contact information "for the purposes of enabling the individual to be contacted in relation to

	the individual's business responsibilities and for no other purpose." In this case, I considered that the possible unauthorized access to the information was not "for the purposes of enabling the individual to be contacted in relation to the individual's business responsibilities and for no other purpose." Therefore, to the extent the personal information was collected in Alberta, PIPA applies in this matter.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On October 1, 2018, an internal investigation revealed suspected malicious code on the Organization's systems. The suspected malicious code may have had the ability to access and acquire information as it was entered onto the payment transaction form used by the Organization's online store. • The potential incident occurred between approximately July 7, 2017 and October 2, 2018. • The Organization cannot confirm that any individual customer's information was in fact involved in the potential incident.
Affected individuals	The incident affected 79,720 companies, including 6 in Alberta
Steps taken to reduce risk of harm to individuals	• A forensic investigation was initiated to determine the extent of the potential security incident. • Suspected malicious code was identified and removed. • Credit card companies were notified. • Customers were notified and advised to monitor their credit records and financial accounts. • A call center was set up allowing customers to have questions answered by professionals familiar with the incident. • Reset administrative accounts, updated software security patches and fixes, and has undertaken to migrate all of its payment functions to PayPal.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter November 6, 2018.

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 potential harms that could result from the breach include "…financial loss or fraud in the form of fraudulent credit card charges." In my view, a reasonable person would consider the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to 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 "There is a risk of harm due to the apparent malicious intent of the third-party attackers and the relative lack of available evidence to concretely understand the nature and scope of the attack." In my view, a reasonable person would consider the likelihood of harm resulting in this case is increased because the incident appears to be the result of deliberate, malicious action. The information may have been exposed for approximately 15 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 the contact and financial information at issue could be used to cause the significant harms of identity theft and fraud. Email addresses could be used for phishing purposes, increasing vulnerability to identity theft and fraud. The likelihood of harm resulting in this case is increased because the incident appears to be the result of deliberate, malicious action. The information may have been exposed for approximately 15 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 the Organization notified the affected individuals by letter November 6, 2018. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner