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	Graphik Dimensions, Ltd. (Organization)
Decision number (file number)	P2017-ND-12 (File #004658)
Date notice received by OIPC	January 4, 2017
Date Organization last provided information	January 4, 2017
Date of decision	January 9, 2017
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 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)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	Some or all of the following information was involved in this incident: • name, • billing address, • full credit card number, expiry date, security code (CVV), and • user name and password. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected in Alberta via the Organization's e-commerce website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• On or around November 9, 2016, the Organization was advised that it had been identified as a common point of purchase for credit card fraud. • On or around November 29, 2016, the Organization's investigation confirmed that an unidentified third party had injected malicious code into the Organization's e-commerce website (pictureframes.com). • The malicious code enabled the unidentified third party to acquire credit card information while purchases took place. • The Organization's investigation revealed that the access occurred between July 12, 2016 and November 30, 2016.
Affected individuals	The incident affected 13 residents of Alberta.
Steps taken to reduce risk of harm to individuals	• Reported the incident to federal law enforcement and notified credit card brands. • Provided customers with information about how to protect against identity theft and fraud. • Notified other regulators and consumer reporting agencies where required.
Steps taken to notify individuals of the incident	Written notice of the incident was mailed to affected individuals on or about December 28, 2016.
REAL RISK OF SIGNIFICANT HARM ANALYSIS	
Harm Some damage or detriment or injury that could be caused to the 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.	In its report of the breach, the Organization did not specifically identify any potential harm that might result to affected individuals from the incident. However, the Organization did advise that it would be "providing its affected customers notice of this incident along with information on how to better protect against identity theft and fraud." In my view, the information at issue could be used to cause the harms of 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 did not assess the likelihood of harm resulting from this incident. In my view, the likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and malicious code) and the information was exposed for over 4 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 information at issue could be used to cause the significant harms of identity theft and fraud. The likelihood of harm resulting from this incident is increased as the breach was the result of malicious intent (deliberate intrusion and malicious code) and the information was exposed for over 4 months. I require the Organization to notify the affected individuals in Alberta in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation). I understand that written notice of the incident, in compliance with the Regulation, was mailed to affected individuals on or about December 28, 2016. The Organization is not required to notify affected individuals again.

Jill Clayton
Information and Privacy Commissioner