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	FitFabFun, Inc., a Delaware corporation (Organization)
Decision number (file number)	P2020-ND-145 (File #015952)
Date notice received by OIPC	June 1, 2020
Date Organization last provided information	June 1, 2020
Date of decision	November 17, 2020
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 based in Los Angeles, USA, and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved some or all of the following information: • customer name, • address, • city, • state, • zip code, • telephone number, • email address, and • credit card number, security code and expiry date. This information is about an identifiable individual 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	• A third party installed malicious code on the shop extension of the Organization's website, using an employee's administrative credentials. • The code was placed on the site on May 2, 2020 and was discovered on May 6, 2020, during a routine review of its website.
Affected individuals	The incident affected 664 individuals, including nine (9) individuals in Alberta.
Steps taken to reduce risk of harm to individuals	• Removed the malicious code from its site and activated its incident response plan. • Conducted an internal investigation and retained advisors to assist in the investigation and response. • Reviewing information security policies and practices. • Conducting a comprehensive review of how the administrative credentials at issue were compromised. • Preparing a mandatory privacy and security training module.
Steps taken to notify individuals of the incident	Affected individuals were notified by letter on May 22, 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 non-trivial consequences or effects.	The Organization reported "As payment card information was involved, it is possible that affected consumers could have fraudulent charges on their credit acocunts [sic]". In my view, a reasonable person would consider that the contact and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. 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.	The Organization reported, *Customers' name, addresses, email addresses, phone numbers, payment card numbers, expiration dates, and CVV codes were potentially compromised. Thus, it is possible that affected consumers could have fraudulent charges placed on their card acocunts [sic].* In my view, a reasonable person would consider the likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Further, it appears the information was exposed for approximately four (4) days.

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 and financial information at issue could be used to cause the harms of identity theft and fraud. Email addresses could be used for the purposes of phishing, increasing vulnerability to identity theft and fraud. These are all significant harms. The likelihood of harm resulting from this incident is increased because the personal information was compromised due to the malicious action of an unknown third party (deliberate intrusion). Further, it appears the information was exposed for approximately four (4) days. I require the Organization to notify the affected individuals whose 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 letter on May 22, 2020 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner