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	Match-Up Solutions LLC (Organization)
Decision number (file number)	P2017-ND-60 (File #003024)
Date notice received by OIPC	May 26, 2016
Date Organization last provided information	May 26, 2016
Date of decision	May 23, 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 online provider of products located in Florida, USA. It is an "organization" as defined in section 1(1)(i)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • address, • credit and debit card number, security code, and expiry date. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. The information was collected from residents of Alberta via the Organization's website.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On May 3, 2016, the Organization learned that online stores it maintained for one of its clients may have been compromised.

	• The Organization investigated and found that one or more unauthorized individuals may have gained access to the e-commerce platform and inserted malware. • The Organization believes that customers' personal information may have been accessed by an unauthorized third party between December 7, 2015 and May 3, 2016.
Affected individuals	A total of 3,078 individuals were affected, including 2 Alberta residents.
Steps taken to reduce risk of harm to individuals	• Immediately took the sites offline. • Hired independent computer forensic experts to investigate. • Instructed affected individuals to monitor their statements and notify their financial institution. • Provided affected individuals with credit monitoring and identity restoration services for 12 months with AllClear ID.
Steps taken to notify individuals of the incident	Affected individuals were notified by email sent on May 26, 2016.
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.	In its report of the incident, the Organization did not specifically identify harms that could result from the incident. However, the Organization reported that "Financial institutions reimburse fraudulent charges upon detection by the financial institution or the cardholder. Additionally, [the Organization] is providing impacted individuals with identity restoration services…". In my view, the financial information at issue (including payment card numbers, security codes and expiry dates) could be used to cause the significant harms of 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.	In its report of the incident, the Organization did not specify the likelihood that harm to affected individuals could result. However, the Organization reported that "Financial institutions reimburse fraudulent charges upon detection by the financial institution or the cardholder." In its letter to affected individuals, the Organization says, "We do not believe you are at risk for identity theft…". In my view, 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 and installation of malware). Further, the information may have been exposed for approximately five months.

	The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

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. The financial information at issue (including payment card numbers, security codes and expiry dates) could be used to cause the significant harms of identity theft and fraud. 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 and installation of malware). Further, the information may have been exposed for approximately five months. The Organization can only speculate that affected individuals will not be held responsible for any credit card fraud and misuse. Even if this were the case, it does not necessarily mitigate the potential harm from identity theft or other forms of fraud.

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 the Organization notified affected individuals in an email dated May 26, 2016, in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner