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	Gyft, Inc. (Organization)
Decision number (file number)	P2016-ND-15 (File #002662)
Date notice received by OIPC	March 31, 2016
Date Organization last provided information	March 31, 2016
Date of decision	July 20, 2016
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"	The incident involved all or some of the following information: • name, • address, • date of birth, • telephone number, • email address, • gift card numbers, and • account credentials. This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	

Description of incident	• The Organization provides an online service and mobile application that allows users to purchase and store gift cards. • Beginning on October 3 and continuing through December 18, 2015, an unknown unauthorized party accessed two cloud providers used by the Organization. • Using valid credentials, the unknown party was able to view or download customer information stored with these cloud providers and make a file containing some of that user information. • The Organization became aware of the incident on December 3, 2015, when it learned that a file available on the Internet appeared to contain user records. It was not immediately apparent how the file had been created. It was not until approximately December 28, 2015 that the Organization discovered its cloud providers had been accessed without authorization. • The Organization has not been able to determine how the credentials were obtained *or* who obtained them.
Affected individuals	The Organization reported that approximately 910 users accessed its site from Alberta, and an additional 290 users accessed its site from an unknown location in Canada.
Steps taken to reduce risk of harm to individuals	• Immediately initiated an investigation. • Forced the reset of user credentials and/or forced logouts for affected users. • The compromised credentials to the cloud accounts were immediately reset when the access was discovered.
Steps taken to notify individuals of the incident	Alberta residents were notified by email starting March 7, 2016. U.S. customers were notified in February 2016, via the Organization's website and in the press.
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 the information at issue could be used to make unauthorized purchases, resulting in financial harm. However, it is likely that in many or most cases, there would be no more than nominal funds on a user's card(s). The Organization noted that there was no access to full credit card numbers, or CCV codes. I agree with the Organization's assessment. The personal information at issue includes sensitive identity and financial information that could be used to cause the harms of identity theft and fraud or financial loss. In addition, the information at

	issue includes email addresses, which could be used for phishing purposes. 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 it "does not believe that the risk of harm is significant" and noted that there is "No evidence that anyone used the information potentially compromised in this incident to access the Organization's accounts or make unauthorized purchases." In addition, the Organization reported that there had not been an increase in successful sign-ins since the incident, suggesting no use of the compromised user credentials. However, the Organization "cannot ensure that cards were not used by unauthorized parties" and noted that "users could have reused the same credentials on other sites." In my view the likelihood of harm resulting from this incident is increased because the incident was a deliberate action by an unknown and unauthorized party, and the information was exposed for approximately two and a half months. The Organization is not able to ensure that cards have not been used by unauthorized parties, and I note that the potential phishing harm has not been mitigated.

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 personal information at issue includes sensitive identity and financial information that could be used to cause the harms of identity theft and fraud or financial loss. In addition, the information at issue includes email addresses, which could be used for phishing purposes. These are significant harms. The likelihood of harm resulting from this incident is increased because the incident was a deliberate action by an unknown and unauthorized party, and the information was exposed for approximately two and a half months. The Organization is not able to ensure that cards have not been used by unauthorized parties, and the potential phishing harm has not been mitigated.

I require the Organization to notify the affected individuals in accordance with section 19.1 of the *Personal Information Protection Act Regulation* (Regulation).

I understand the Organization notified the affected individuals by email on March 7, 2016 in accordance with the Regulation. The Organization is not required to notify the affected individuals again.

Jill Clayton
Information and Privacy Commissioner