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	Omaze, Inc. (Organization)
Decision number (file number)	P2021-ND-290 (File #018030)
Date notice received by OIPC	November 4, 2020
Date Organization last provided information	January 31, 2021
Date of decision	April 5, 2022
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 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 reported that it is "an American based multinational company offering a fundraising platform which benefits charities by offering individuals the chance to win various forms of experiences as prizes." The Organization is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	The incident involved all or some of the following information: • name, • email address, • username, • gender, • country, zip or postal code, and • links to individual's public social media profiles (where provided by the user). The Organization reported that "no financial information or otherwise sensitive information has been identified as compromised", but that "…approximately 200,000 of these records also contained hashed passwords of user accounts for a legacy … platform (a site that is no longer active)."

	This information is about identifiable individuals and is "personal information" as defined in section 1(1)(k) of PIPA. To the extent the personal information was collected in Alberta, PIPA applies.
DESCRIPTION OF INCIDENT	
❑ loss ☒ unauthorized access ❑ unauthorized disclosure	
Description of incident	• On October 8, 2020, the Organization was notified by the Federal Bureau of Investigation that it had potentially been subject to a cyber-attack, and a database of what was purported to be the Organization's user data was available on a sharing and marketplace forum. • The Organization reported that it appears the records were posted to the forum on July 19, 2020. • The Organization identified that the posted database contained two datasets of purported user information, which appeared to have been obtained from a legacy database hosted in a cloud environment provided by Amazon Web Services (AWS). • The Organization believes that the intruders obtained credentials for one of its employees, and exploited those credentials to access the database.
Affected individuals	The Organization reported the incident involved two compromised datasets which "...consisted of a total of 2,803,024 records". The incident affected approximately 207 residents of Alberta with emails and hashed password, and 3,300 residents of Alberta with emails without hashed password.
Steps taken to reduce risk of harm to individuals	Investigated and took immediate actions to download and analyze the exposed database.
Steps taken to notify individuals of the incident	The Organization reported affected individuals had not been notified.
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	With respect to the harm(s) that might result to affected individuals as a result of this incident, and hashed passwords in particular, the Organization said: *To date, the forensic vendor has completed its examination into the quality of the hashing on the passwords contained in the compromised databases. Based on its independent analysis, the forensic*

non-trivial consequences or effects.	*vendor concluded that all of the passwords contained in the compromised databases were hashed with a robust encryption, that complies with industry standards for password encryption, rendering them unreadable and unusable to the unauthorized persons.* *… Now, based on the finding of the third-party forensic investigation that the passwords were completely encrypted, it seems that the real risk of significant harm threshold is not met.* In my view, given the passwords were "completely encrypted", a reasonable person would consider that the hashed passwords at issue could not be used to cause any significant harm. With respect to the email addresses at issue, the Organization's submission appears to recognize that email addresses could be used for phishing purposes and to make unsolicited requests for donations: *[The Organization] is of the view that a reasonable person would understand that it is not uncommon to publicize the connection between an individual in the charitable and non-profit sectors and an organization. Further, a reasonable person would also understand that unsolicited requests for donations are common (and, indeed, this permitted [sic] under Canada's Anti-Spam Legislation). Accordingly, a reasonable person would take some precautions to protect themselves from phishing emails in the guise of donation requests by checking charitable registration numbers and information provided by the sender before making a donation.* I agree with the Organization. In my view, a reasonable person would consider that email addresses, particularly when combined with additional information (for example, that an individual is associated with a particular organization), could be used to send sophisticated, user-specific phishing emails purportedly from the Organization. If an individual believed the email came from a trusted organization, the individual could be prompted to provide additional personal information or even credentials, increasing vulnerability to identity theft and fraud. Merely clicking on a link, without a user providing any additional information, could potentially activate malware or infect users' computer/networks. These are significant harms. This finding is consistent with numerous breach notification decisions issued by my office, as far back as 2011. For example, in

	breach notification decision #P2011-ND-011, the former Commissioner said: *A successful phishing attempt may persuade victims to disclose sensitive personal information that can then be used for theft, fraud, identity theft or other criminal acts, or where a malware install is successful, can do any number of things to an affected computer. All of these possibilities are, in my view, 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.	I have already said above that, in my view, a reasonable person would not consider that "completely encrypted" hashed passwords could be used to cause any significant harm. With respect to the likelihood of email addresses being used to cause significant harm, however, the Organization reported: *While [the Organization] appreciates that the OIPC has concluded that there could be an increased risk of successful phishing as a result of the unauthorized access or disclosure of contact information (particularly emails), it is [the Organization's] position that each situation must be examined in context from the perspective of a reasonable person (not an unusually sensitive or inexperienced individual). [The Organization] is of the view that a reasonable person would understand that it is not uncommon to publicize the connection between an individual in the charitable and non-profit sectors and an organization. Further, a reasonable person would also understand that unsolicited requests for donations are common (and, indeed, this [is] permitted under Canada's Anti-Spam Legislation). Accordingly, a reasonable person would take some precautions to protect themselves from phishing emails in the guise of donation requests by checking charitable registration numbers and information provided by the sender before making a donation.* *Given this context and the fact that [the Organization] is unaware of any evidence that the information has been actually used for phishing, it would appear that the risk is speculative and a finding that the real risk of significant harm has been met would depend on the Commissioner making a number of assertions not grounded in any evidence. Accordingly, it is [the Organization's] position that the disclosure of the email addresses alone, given these facts, should not be found to meet the threshold of a "real risk of significant harm" and should not trigger*

	consumer notification. This conclusion and result would be consistent with the result in other jurisdictions in which [the Organization] has reported this incident. The Organization also advised that "…the federal OPC has agreed with [the Organization's] position that there is no real risk of significant harm in this case…namely, that there was only contact information exposed in the incident because the passwords were sufficiently encrypted." And further... *…on the same facts, the U.K.'s ICO …will not require consumer notification in this circumstance. The ICO stated it would close its file without taking further action because, inter alia, "…the incident affected a relatively low number of UK Data Subjects, and the nature of the compromised data means that the risk to those data subjects is low."* The Organization also said that … *… as an international organization, [the Organization] is striving to apply standards from multiple jurisdictions. As such, we feel that it is important for the Canadian regulators to consider the international response to this incident when determining [the Organization's] obligation to notify affected individuals. It seems that the international data protection authority community should work to create interoperable rules – not those that would promote unworkable and differing standards from one jurisdiction to another.* To summarize, having reviewed the Organization's submissions, I understand the Organization to be saying that, despite the fact email addresses could be used for phishing purposes, there is no real risk of significant harm in this case because: • It is not uncommon to publicize the connection between an individual in the charitable and non-profit sectors and an organization; • a reasonable person would understand that unsolicited requests for donations are common; • a reasonable person would take some precautions to "protect themselves from phishing emails …by checking charitable registration numbers and information provided by the sender before making a donation";

	• the Organization is not aware of any phishing emails resulting from this incident; and • other jurisdictions have decided that "only contact information" was exposed, the incident affected "a relatively low number of data subjects" in those other jurisdictions, and the various data regimes should be "consistent and more interoperable". I do not accept the Organization's argument. In my view, a reasonable person would consider the likelihood of significant harm resulting from this incident is increased because the personal information was compromised due to the deliberate, malicious action of an unknown third party (intruders obtained employee credentials, exploited those credentials to access the database and posted the information on a public forum). The incident affected over 2 million records, including 3,000+ residents of Alberta. It appears the information may have been exposed for approximately three months before the Organization became aware of the breach. The lack of reported incidents to date does not mitigate against future harms, as phishing, fraud and identity theft can occur months and even years after a data breach. Individuals will be particularly vulnerable to significant harm if they receive a targeted phishing email that appears to be from an organization with whom they have a relationship. If they are aware their information was involved in a malicious incident and made public, they will be more likely to take the precautionary steps the Organization describes in order to protect themselves. I acknowledge the Organization says regulators in other jurisdictions found "there is no real risk of significant harm" because "only contact information [was] exposed in the incident because the passwords were sufficiently encrypted" and "the incident affected a relatively low number of UK Data Subjects". As such, the Organization believes my decision should be "consistent" and "interoperable" with these other jurisdictions. In my view, this argument is not relevant. I am not privy to the reports that were made to other regulators, the circumstances of the breach (i.e. how many individuals were affected), and I do not know the specifics of their laws nor the exact reasons for any decisions made. I do not find the Organization's submission on the need for "interoperability" to be relevant to a determination of whether there is a real risk of significant harm to affected individuals whose personal information was collected in Alberta. I also do not see how a decision that there is a real risk of significant harm to these individuals would not be "interoperable" with a decision concerning individuals in another jurisdiction.

	With respect to the Organization's argument for "consistency", I note that the reasoning behind my finding in this case is consistent with the reasoning in previous decisions issued by my office, dating as far back as 2011. For example, in breach notification decision #P2011-ND-011, the former Commissioner said: *In my opinion, the foreseeability of fraud or identity theft as harms that may arise from the ...breach is not mere speculation or conjecture. There is a clear cause and effect relationship between the potential harm that may arise ... Affected individuals are likely to be targeted with "spear phishing" emails which directly target them as known customers of [the organization]. It is to be hoped that most individuals will ignore these emails, particularly so in cases where they have received notification of the breach and potential risks. However, a small (it is hoped) portion of affected individuals are likely to either open attachments with malware or be tricked into providing additional information. This is the known pattern that is used by criminals when attempting to obtain personal information. Phishing attempts have been successful in the past and there is no evidence to indicate that the information obtained through the ...breach will be treated any differently.* *[21] In this case, two factors in particular are relevant to my assessment of whether a "real risk" exists. These are 1) the magnitude of the ....breach and the number of affected ... customers and 2) the sophistication of the attack and the belief that [the organization] was targeted for nefarious purposes. The... breach was not an accidental loss or disclosure of personal information; it was a targeted attack to obtain personal information. This is a critical fact in my evaluation of the real risk in this situation. It is a well-known fact that identity theft and fraud are a booming business for organized crime and in the circumstances of this case, it is reasonable to assume that [the organization] was targeted for nefarious purposes.* Similar to the former Commissioner's deliberations, I have considered the specific facts of this case: the type of information and potential harms, the fact the breach resulted from deliberate, malicious action, the number of affected individuals, the fact the information was posted publicly and the length of time the personal information was exposed.

	All of these case-specific factors lead me to conclude that a reasonable person would consider this incident gives rise to a real risk of significant harm to affected individuals.

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 whose personal information was collected in Alberta.

In my view, given the passwords were "completely encrypted", a reasonable person would consider that the hashed passwords at issue could not be used to cause any significant harm.

Email addresses, however, particularly when combined with additional information (for example, that an individual is associated with a particular organization), could be used to send sophisticated, user-specific phishing emails purportedly from the Organization. If an individual believed the email came from a trusted organization, the individual could be prompted to provide additional personal information or even credentials, increasing vulnerability to identity theft and fraud. Merely clicking on a link, without a user providing any additional information, could potentially activate malware or infect users' computer/networks. These are significant harms.

The likelihood of significant harm resulting from this incident is increased because the personal information was compromised due to the deliberate, malicious action of an unknown third party (intruders obtained employee credentials, exploited those credentials to access the database and posted the information on a public forum). The incident affected over 2 million records, including 3,000+ residents of Alberta. It appears the information may have been exposed for approximately three months before the Organization became aware of the breach. The lack of reported incidents to date does not mitigate against future harms, as fraud and identity theft can occur months and even years after a data breach. Individuals will be particularly vulnerable to significant harm if they receive a targeted phishing email that appears to be from an organization with whom they have a relationship. If they are aware their information was involved in a malicious incident and made public, they will be more likely to take the precautionary steps the Organization describes in order to protect themselves.

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).

The Organization is required to notify the affected individuals in Alberta in accordance with section 19.1 of the Personal Information Protection Act Regulation (Regulation) and confirm to my Office in writing, within ten (10) days of the date of this decision, that it has done so.

I am aware that the Organization reported that "...it does not have good location data associated with the email addresses at issue. In the tables at issue, location data either does not exist at all, was user inputted and unverified, or may have been inferred from other information."

If the Organization is asserting that, in the circumstances, it is not possible or is impracticable to notify affected individuals whose personal information was collected in Alberta directly, it may apply to me for authorization to meet its legal obligations in some other manner (for example, through indirect or substitute notice).

Jill Clayton
Information and Privacy Commissioner