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	2364920 Alberta LTD. o/a PORTpass Inc. (Organization)
Decision number (file number)	P2021-ND-232 (File #023369)
Date notice received by OIPC	October 6, 2021
Date Organization last provided information	November 15, 2021
Date of decision	November 19, 2021
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's website describes it as the creator of "...the PORTpass app to help users access and to securely store and share only their proof of vaccine health status and their COVID-19 test results". The Organization operates, and is headquartered, in Calgary, Alberta, and is an "organization" as defined in section 1(1)(i) of PIPA.
Section 1(1)(k) of PIPA "personal information"	This incident involves information collected by the Organization that was inadvertently made accessible to the public. The Organization initially described the information at issue as follows: *If the information would have been looked at, not taken from an end-point or a url - it would have been someones name, phone number, perhaps their ID if it was on their profile that was awaiting to be verified.* In response to questions and in subsequent submissions received between October 11, 2021 and November 15, 2021, the Organization said:

	• "The majority of the accounts were just an email address (16) and the (15) were name, phone - Many of the accounts had optional for PHN but were not filled for the most part." • "15 unauthorized viewers for Identifications, name and birthdays. The Blood type option and PHN option." • "Certain individuals only had their email address, some their name and some more information." • "Based on what we know, there was no licenses/passports/nexus/status cards on file … nor was there the fields of PHN or blood type…We would not have had those open, especially since we had disabled and removed the PHN/blood type on our backends." • "As per the [news] article, the IDs that were unauthorized viewed and were controlled through the viewing process could have been of the any [sic.] as a user could have utilized that for their verification process." • "blood type (optional), PHN (optional), IDs, name, DOB, Phone number and postal code as well as the users email address." I note that media reports of the incident said[1]: *... email addresses, names, blood types, phone numbers, birthdays, as well as photos of identification like driver's licences and passports can easily be viewed by reviewing dozens of users' profiles.* Given the above, it appears the incident may have involved all or some of the following information: • name, • telephone number, • email address, • personal health number, • blood type, • drivers licence, • passport, • Nexus Card, • Indian Status Card, • vaccination record, and • COVID-19 test result.

[1] CBC News, retrieved from https://www.cbc.ca/news/canada/calgary/portpass-privacy-breach-1.6191749

	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	• The Organization initially reported that, on September 27, 2021, it was notified by a journalist about a "vulnerability on our end-point of a url that was hidden on the web portal version ...". • The breach occurred when the Organization's "external team" was "adding various end-to-end encryption on the web portal version on AWS for users that don't have mobile phones for the app". • The Organization reported that it turned off its server "within 5 minutes of being notified" of the breach and "The inappropriate access seems to have happened between the nine-hour window of 27 Sept 18:21:49 UTC and 28 September 2021 03:07:13 UTC". • On October 28, 2021, the Organization contacted my office to "speak about another alleged unauthorized viewing". The Organization provided additional information on November 4, 2021, consisting of excerpts of a security audit that cited logs showing an unauthorized third party accessing or trying to access user profiles on October 17, 2021. • The Organization explained that unauthorized actors could view users' personal information by navigating to "deeply hidden" URLs. • The Organization did not report how long the personal information was exposed. • Both incidents were made public by way of news articles published by the CBC on September 28 and October 28, 2021.
Affected individuals	The Organization initially reported that "7 to 31 (at maximum unverified users) User records were likely inappropriately accessed", and noted that some accounts were "test" accounts, others "did not have first or last names entered" or "did not have a value for 'id_card_image'". The Organization later reported the affected individuals as "31 Total. 16 with no names, just email addresses only, 15 with names and ID. *51 total viewed but were dummy/test/bogus accounts."

	Despite this, I note that a CBC News report said that the media outlet "... was able to independently confirm that the records of more than 17,000 users were still unsecured after the relaunch". When questioned about this report, the Organization confirmed that "17,541 is the total to date of users ... that we have on our app. This can be one time sign ups, half set up registered or using users." When asked whether the Organization could rule out the possibility that the information of those 17,541 users was accessible, the Organization responded: > ***The potential could have been there,*** *however it was not accessed due to the fact what the iteration test was only able to see the total numbers of individuals, not the actual individuals accounts, just a total number. [emphasis added]* Despite the Organization's response, I note the CBC reported it "...was able to view text-based data showing users' names, phone numbers, email addresses, dates of birth, vaccination status and, in some cases, Alberta health-care numbers."
Steps taken to reduce risk of harm to individuals	• Turned the server off "within 5 minutes of being notified" of the initial breach. In respect of the second incident, the Organization said "The unauthorized potential were container [sic] and the vulnerability has been addressed and reviewed/modified by our team." • Removed the service's front-end web portal. • Deactivated affected user accounts. • Retained a cybersecurity firm and auditors "to see the damage". • Added a bug bounty. • Implemented authentication requirements. • Enhanced monitoring and vulnerability scanning. • Created "crisis management measures" as well as policies and procedures. • Switched development companies. • Notified police. • Offered credit monitoring to affected individuals.
Steps taken to notify individuals of the incident	The Organization reported that it notified 31 affected individuals by email between October 8 and 10, 2021. However, the notices do not appear to contain a description of the affected personal information and therefore do not meet the requirement of section 19.1(1)(b)(iii) of the Regulation.

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 did not specifically identify potential harms that could be caused to affected individuals as a result of this incident, but initially reported: *The harm was that the CBC reporter and the accomplice were the two individuals that looked and notified us - we shut off our server from being live immediately.* The Organization subsequently reported: *The harm that may have occurred is the unauthorized viewings, however from the third-party audit reports, we noticed thankfully that no data harvesting or mining was done – just an unauthorized viewing of a url that had to be found manually.* On October 28, 2021, the Organization said: *The personal harm that could occur was done in regards to test the weaknesses in our system which we have addressed with our team … if the information in the wrong hands did happen, it would not be appropriate, however we have looked into the IP addresses and realized what exactly was happening.* On November 4, 2021, the Organization said: *The harms could have been severe if they were in the hands of the wrong people and as what our cybersecurity firm that we brought on has evaluated was that this could have been harmful, however the viewing was done professionally by the CBC and the security/it/web individuals to see if our [system] had any vulnerabilities, which we have addressed and fixed.* In my view, a reasonable person would consider that the identity (driver's license, PHN, passport, etc.), contact, and medical information (vaccination status, COVID-19 test result) that may be at issue could be used to cause the harms of fraud, identity theft, and possibly embarrassment. Email addresses could be used for the purposes of phishing and/or spear-phishing, increasing affected individuals' vulnerability to 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.	In assessing the likelihood of significant harm resulting from this incident, the Organization initially reported: *The harm was reduced and we notified the team that was looking after the app and web portal to make sure no updates are ever done live. The harm was thankfully not taken in regards to an individual's identity nor was an [sic] user profiles hacked, back end hacked or user profile scripts harvested. The profiles that may have been seen were to show us that we were editing a token live and it would have taken the individual from Calgary (ip address) manually to randomly pick/ see unverified information of users that were not verified yet in our AWS web portal system.* *We have brought on 2 cybersecurity firms to help us audit each time a test, update and anything is completed. We have brought on a firm to help us ensure to the public with compliance and are in talks with various government officials and figures of authority to help us with further guidelines so we as a growing startup can help people return to work or do their favourite things in a safe manner.* *Currently, our web server is still done and we have not turned it on as we wanted to get more penetration tests done, get our organization to complete the checklist for PII, SOC 2 and HIPAA compliance as well.* The Organization later reported: *The harm thankfully was mitigating [sic] and eliminated immediately. However, maybe the viewing primarily to the reporter seeing the randomly typed in end-point urls to see the unverified portpass users profile.* In a further communication on October 28, 2021, the Organization said: *No malicious attacks conquered [sic.] as the data was not gather [sic] to hurt the user, the data was viewed by trying to find weaknesses in the portpassportal.com system which was identified in the articles by the [reporter].* *The above likely harmed would be that the [reporter]/IT professionals may have looked at their information to see where the weak points may have been on our web portal.*

	Finally, on November 4, 2021, the Organization said: > *[The] viewing was done professionally by the [media] and the security/it/web individuals to see if our [system] had any vulnerabilities, which we have addressed and fixed.* In determining whether a reasonable person would consider there is a real risk of significant harm resulting from this incident, I note that the likelihood of harm is decreased because the personal information was compromised due to human error – failure or lack of adequate technical and/or administrative safeguards – and not malicious intent. It is also unlikely that the CBC representatives who accessed and viewed the information online would use the information to cause significant harm to individuals. Nonetheless, despite the Organization reporting that measures were taken after the first incident to prevent similar incidents from occurring, it appears personal information was publicly disclosed on at least two occasions. The Organization did not confirm exactly how long the information at issue was exposed as a result of the two incidents. The Organization did confirm that some information was in fact accessed by unauthorized parties (media representatives). One of these representatives also reported receiving "a tip" from "a third person anonymously … detailing how they were able to access user data, as well." The same article confirmed that "… the records of more than 17,000 users were still unsecured after the relaunch. The confirmation was done by using an automated script to scan the information that was accessible online without storing all of the users' personal information." When questioned whether it could rule out the possibility that the information of all 17,541 users was accessible, the Organization responded: > ***The potential could have been there,*** *however it was not accessed due to the fact what the iteration test was only able to see the total numbers of individuals, not the actual individuals accounts, just a total number. [emphasis added]* Despite the Organization's response, I note the CBC reported it "...was able to view text-based data showing users' names, phone numbers, email addresses, dates of birth, vaccination status and, in some cases, Alberta health-care numbers."

	Overall, media reports describing the information that was publicly accessible are not consistent with what the Organization reported to my office. When these discrepancies were put to the Organization with a request to clarify, the Organization's explanations were inconsistent, at times incomplete, and were not reassuring. Given the unresolved discrepancies concerning the information at issue, the number of potentially affected individuals, the identities and number of third parties who may have accessed the information online, the fact of the two incidents, and the unknown length of exposure, I conclude that a reasonable person would consider there is a real risk of significant harm in this case to the 17,541 potential 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.

A reasonable person would consider that the identity (driver's license, PHN, passport, etc.), contact, and medical information (vaccination status, COVID-19 test result) that appear to be at issue could be used to cause the harms of fraud, identity theft, and possibly embarrassment. Email addresses could be used for the purposes of phishing and/or spear-phishing, increasing affected individuals' vulnerability to identity theft and fraud. These are significant harms.

Given the unresolved discrepancies concerning the information at issue, the number of potentially affected individuals, the identities and number of third parties who may have accessed the information online, the fact of the two incidents, and the unknown length of exposure, I conclude that a reasonable person would consider there is a real risk of significant harm in this case to the 17,541 potential affected individuals.

I understand the Organization notified 31 affected individuals by email on or about October 8 and October 10, 2021; however, it is not clear the notice complied with the requirements of section 19(1)(b)(iii) of the Regulation. Further, the Organization did not notify all of the 17,541 affected individuals who are potentially at risk of significant harm.

I require the Organization to notify all affected individuals whose personal information was collected 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 individuals have been notified of this incident in accordance with the requirements outlined in the Regulation.

Jill Clayton
Information and Privacy Commissioner