Office of the Information and
Privacy Commissioner of Alberta

Investigation Report P2022-IR-02

***Investigation into PORTpass' protection of personal information under the* Personal Information Protection Act**

July 28, 2022

PORTpass

Investigation 023334

Commissioner's Message

Organizations collecting, using or disclosing personal information have a duty to protect records in their custody or under their control. When the records include medical and identity information, the importance of protecting personal information against threats and reasonably anticipated risks increases.

PORTpass claimed, via its website and privacy policy, to protect personal information by implementing encryption and blockchain technology. Such claims may be compelling, particularly at a time when organizations and individuals wanted an immediate digital solution for proving vaccination. We were not, however, able to substantiate any of PORTpass' claims about how it protected personal information. During this investigation, PORTpass failed to demonstrate that it implemented any technical and administrative safeguards to protect personal information.

Additional assurances from PORTpass that steps had been taken to securely destroy personal information were also unreliable. There were no responses to follow up questions about the destruction of personal information. It was also unclear whether PORTpass took other corrective measures.

Overall, this investigation serves as a reminder to customers and business clients alike.

Everyone must exercise caution and, where possible, verify that organizations deliver on privacy and security promises prior to consenting to the collection, use or disclosure of personal information. When startups can disappear as suddenly as they appear, building trust with organizations can be challenging. Taking a few minutes to research an organization before deciding whether to accept the terms and conditions can go a long way.

Likewise, organizations contracting or subcontracting services ought to assess the privacy and security controls of prospective contractors – for example, by way of a privacy impact assessment – to understand and mitigate potential risks to customer privacy and organizational reputation.

Jill Clayton
Information and Privacy Commissioner

Table of Contents

Background

[1] On September 26, 2021, CBC News published an article concerning PORTpass (or Portpass), describing it as a "... Calgary-based company... [with] more than 500,000 users across Canada registered for its app, which is touted as a way to store and share vaccine records and COVID-19 test results."[1]

[2] The article said, "The Calgary Sports and Entertainment Corporation (CSEC) has recommended the app for getting into NHL and CFL games in the city. Alberta currently does not have a proof-of-vaccination app, but the government has said it plans to create a QR code."

[3] The article also described a number of "privacy, security concerns" with the PORTpass app, including reports that its website could be used to create fake vaccination records, and "... does not appear to validate security certificates and has a backend that can easily be accessed by members of the public — making its data potentially vulnerable to hackers."

[4] The article was updated on September 28, 2021 to say, "Private proof-of-vaccination app Portpass exposed personal information, including the driver's licences, of what could be as many as hundreds of thousands of users by leaving its website unsecured."[2]

[5] That same day, the Office of the Information and Privacy Commissioner (OIPC) contacted PORTpass to advise it of its privacy breach reporting responsibilities under section 34.1 of Alberta's *Personal Information Protection Act* (PIPA).

[6] On October 3, 2021, the Information and Privacy Commissioner (Commissioner) received an email from an individual concerning PORTpass' compliance with PIPA. The email said, in part:

> A few days ago, the Portpass App developed in Alberta to house vaccination information was found to be seriously flawed and personal information of thousands of Albertans was in jeopardy of being misused. [Apparently, incidents] of this nature are supposed to be reported to your office, however, the CBC reported a few days ago that the developer had not reported this matter.
>
> As a senior who blindly trusted this app to house my vaccination information, I am highly concerned about identity theft since this app has a copy of my driver's license.

[7] On October 5, 2021, I contacted this individual to discuss their concerns. The individual responded to my initial email, but did not reply to subsequent communications or file a formal complaint, advising instead that:

> My main concern in contacting your office was to ensure that the developer had reported the incident and that the Province of Alberta was taking whatever steps are necessary to ensure that the developer does not misuse the information he collected.

---

[1] Rieger, Sarah. "Private vaccine verification app Portpass sparks privacy, security concerns". September 26, 2021, CBC. Retrieved from https://www.cbc.ca/news/canada/calgary/portpass-security-concerns-1.6190403.

[2] Rieger, Sarah. "Portpass app may have exposed hundreds of thousands of users' personal data". September 28, 2021. Retrieved from https://www.cbc.ca/news/canada/calgary/portpass-privacy-breach-1.6191749.

[8] On October 6, 2021, PORTpass submitted a privacy breach report to the Commissioner. It submitted an updated report with additional information on October 11, 2021. The OIPC opened file #023369 and I was assigned to follow up with PORTpass.

[9] On October 7, 2021, the OIPC received a formal complaint from another individual regarding PORTpass. The complainant identified the matter for review/investigation as, "My personal/health information has been disclosed in contravention of Alberta's privacy laws", and attached a letter that said:

> This letter summarizes the details of a potential privacy breach of my personal information, involving the software company that created the Portpass App. The App is used to show confirmation of vaccination status when attending sporting events and was recommended for use by the Calgary Sports and Entertainment Corporation (Calgary Flames) for entrance to hockey games.
>
> On September 23, 2021, I set up an account on the Portpass website (Portpass.ca) using my computer so that I could use the App to attend Flames games. To set up the account I was required to upload my original documents showing proof of vaccination, a copy of my driver's license, and a photo of myself. Although optional, I also provided my Alberta Health Care number to the website.
>
> Once the account was set up, I then downloaded the App on my Android phone and tried to log in to my account. I kept receiving a message stating that 'you must use a valid e-mail address' and could not log in. I contacted the support team at Portpass and they advised that an update for Android was launching any hour. I kept checking but no updates were forthcoming.
>
> On September 25, 2021, I read in the weekend edition of the Calgary Sun that [there] may have been a privacy breach in relation to the Portpass App which had been recommended for use by the Calgary Flames. On September 27, 2021 I contacted the Calgary Flames to see what was going on with the App. On September 28, 2021, they responded to my request. They advised me that the App was offline for the time being and that I should show hard copy proof of vaccination for now when attending Flames games.
>
> On October 6, 2021, I read in the Calgary Sun that the Calgary Police Service (CPS) had launched an investigation into this matter and that anyone that believes their privacy had been breached should contact the CPS non-emergency line. I contacted them on October 7, 2021 and met with an officer. He took my name and other information and have been added to a list with the case CA#21396094.
>
> At the suggestion of CPS, I also reached out to Portpass on October 7, 2021 to see if they have advised their users of a potential privacy breach, and what steps they are taking to rectify the matter. I received a reply from Portpass the same day and they advised me that according to their records my privacy had not been breached. They also said they would be issuing a public statement shortly to [assure] the public of the measures they have taken and clear the story.

[10] The OIPC opened complaint investigation file #023334, and I was assigned to the matter.

[11] On November 19, 2021, after a series of attempts to clarify and obtain more information from PORTpass, the Commissioner issued breach notification decision P2021-ND-232.[3] The decision described two privacy incidents involving the unauthorized disclosure of personal information in

[3] Office of the Information and Privacy Commissioner. Breach Decision P2021-ND-232. Retrieved from https://oipc.ab.ca/wp-content/uploads/2022/05/P2021-ND-232.pdf.

PORTpass' control, one that occurred on or about September 27, 2021, and another that occurred on or about October 17, 2021.

[12] The decision confirmed that a reasonable person would consider that there exists a real risk of significant harm to affected individuals as a result of the incidents. It said that PORTpass reported it had notified some affected individuals of the breach, but "it is not clear the notice complied with the requirements of section 19(1)(b)(iii) of the [PIPA] Regulation. Further, the Organization did not notify all of the 17,541 affected individuals who are potentially at risk of significant harm."

[13] The Commissioner's decision required PORTpass "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."

[14] PORTpass did not provide written confirmation within the 10-day period, and did not respond to repeated follow-up efforts to obtain written confirmation. However, in a telephone conversation on November 29, 2021, PORTpass' CEO said notifications were being delivered in batches starting on November 25, 2021, and said PORTpass would provide an update on December 1, 2021; PORTpass did not, however, provide the update.

[15] Instead, in an email response on December 6, 2021, PORTpass' CEO reported that, with respect to the individual who had complained to the OIPC, "the issue had been resolved" and a "third-party cyber security audit" confirmed the complainant "was not on the list nor was his email address."

[16] On January 19, 2022, despite PORTpass' verbal report that affected individuals were notified of the privacy breaches beginning on November 25, 2021, the Commissioner again wrote to PORTpass requesting written confirmation that it had complied with the breach notification decision. PORTpass did not respond.

[17] On February 18, 2022, after repeated efforts to contact PORTpass, PORTpass responded to an email request for information. During a subsequent telephone conversation, PORTpass' CEO again verbally confirmed that PORTpass had completed the required notifications to affected individuals as per the breach notification decision.

[18] PORTpass also advised it was no longer operating (in tandem with the Government of Alberta ending the Restrictions Exemption Program) and had subsequently "removed the database" containing personal information. PORTpass also committed to reporting back to the OIPC on February 22, 2022 to provide further clarification.

[19] PORTpass did not report back to the OIPC on February 22. That same day, the OIPC confirmed via CORES search that PORTpass had legally dissolved on or about February 8, 2022.[4]

[4] Alberta's Corporate Registry System is available at https://cores.reg.gov.ab.ca/.

[20] As PORTpass is now dissolved, there is no longer an “organization” as defined in PIPA to whom the Commissioner can make recommendations, or against whom an order compelling compliance can be issued.

[21] I made repeated attempts to obtain information from PORTpass for this investigation. As PORTpass did not provide adequate responses before dissolving, I completed my investigation based on the limited information made available to me, along with open-source research.

[22] This report sets out my findings.

PORTpass

[23] At the time this investigation was commenced, PORTpass' website included an "Our Story" page that described the PORTpass app as follows:

> Our team of developers, designers, business leaders and healthcare professionals in Calgary, Alberta, Canada has created 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 to satisfy the guidelines and standards set for work, travel, dining, sporting and live events province-to-province across the nation of Canada while meeting the standards and access requirements by protecting the users' health privacy and data security at the highest level.[5]

[24] PORTpass submissions for this investigation also said: "We operate as a third-party verifier so that the user can **show their image with their QR code or their [vaccination or COVID-19 test] status** colour of green, yellow or red with a check mark upon entering a facility/event or place of work." [emphasis added]

[25] PORTpass' website described how individuals register and use the app.[6] It read:

> STEP 1
> Visit the PORTpassTM web portal at portpassportal.com or download the IOS/Android mobile app.
>
> STEP 2
> Answer a few questions to confirm your vaccine or test information to retrieve your PORTpassTM.
>
> STEP 3
> Our AI will review and verify your credentials for validation. Print your QR (MapleCode) by PORTpassTM, [sic] or download the free Wallet IOS/Android App to store your PORTpassTM on your phone [sic]
>
> STEP 4
> Present your PORTpassTM and it's [sic] secured 2D Visible Digital Seal QR MapleCode at participating organizations to verify your proof of vaccination or negative test result.
>
> PORTpass™ is a voluntary platform. Your data and information is kept secure at all times and never stored once your account is verified.

[26] Steps 1 and 2 were corroborated by the complainant, who reported, in part:

> On September 23, 2021, I set up an account on the Portpass website (Portpass.ca) using my computer so that I could use the App to attend Flames games. To set up the account I was required to upload my original documents showing proof of vaccination, a copy of my driver's license, and a photo of myself. Although optional, I also provided my Alberta Health Care number to the website. [emphasis added]

[5] PORTpass Inc. "About Us", n.d. Retrieved from https://portpass.ca/about/ on November 17, 2021.
[6] PORTpass Inc. "For Users", n.d. Retrieved from https://web.archive.org/web/20210922234709/https://portpass.ca/for-users/ on June 10, 2022.

[27] After registration and "verification," individuals received a "PORTpass" as defined in "STEP 3." I understand "PORTpass," in this context, to be a record containing an individual's photograph and information conveying the individual's COVID-19 vaccination or test status.

[28] Per "STEP 4," organizations could choose to accept an individual's "PORTpass" as "proof of vaccination or negative test result" in compliance with COVID-19 entrance requirements / protocols. Organizations could view the individual's "PORTpass" as presented via the app or in printed form.

[29] The website further explained that PORTpass "software for organizations allows them to control, manage and **scan** without any hardware required – just their mobile device and/or a computer at a hand." [emphasis added][7]

Launch and Operational Period

[30] It is not clear when the PORTpass app was officially launched. However, a review of open-source media suggests individuals were "pre-registering" to use PORTpass as early as June 14, 2021.[8]

[31] A CTV News article indicates that, as early as September 22, 2021, the Calgary Sports and Entertainment Corporation (CSEC) was advising patrons of plans to use PORTpass as proof of COVID-19 vaccination result prior to permitting access to events.[9] An archived version of the CSEC "Proof of vaccination is required to attend games" webpage reads in part:[10]

> What documentation is accepted for COVID-19 proof of vaccination?
>
> The following documentation will be accepted:
>
> **Preferred & Fastest** - For the most efficient entry possible, all ticket holders should sign up and download **PORTpass** and complete their COVID-19 proof of vaccination online or through the app. A photo, green check mark indicating fully vaccinated, and a QR code will be displayed from the app - no photo identification at entry gates required.
>
> The Province of Alberta's printable vaccination card (printed hard copy or saved on a mobile device) verified with photo identification at entry gates. Vaccination cards are available at **https://www.albertavaccinerecord.ca/**
>
> …
>
> What is PORTpass?
>
> PORTpass is a Made-In-Calgary application that provides a solution for safely and securely sharing vaccine health status for access requirements while protecting user health privacy and data security

[7] PORTpass Inc. "Solutions". n.d. Retrieved from https://web.archive.org/web/20210929010132/https://portpass.ca/solutions/ on June 10, 2022.
[8] PORTpass. "Over 200,000 Canadians pre-registered for Canada's PORTpass™ mobile app for international travel standards and guidelines". June 14, 2021. CISION. Retrieved from https://www.newswire.ca/news-releases/over-200-000-canadians-pre-registered-for-canada-s-portpass-tm-mobile-app-for-international-travel-standards-and-guidelines-809636390.html.
[9] Gilligan, Melissa. "How to prove you're vaccinated at Calgary Flames, Stampeders and Hitmen games". September 22, 2021. CTV News Retrieved from https://calgary.ctvnews.ca/how-to-prove-you-re-vaccinated-at-calgary-flames-stampeders-and-hitmen-games-1.5596532.
[10] Calgary Sports and Entertainment Corporation. Retrieved from https://web.archive.org/web/20210923000058/https://www.nhl.com/flames/fans/vaccination-policy.

at the highest level. With a user base of 500,000+ across Canada, PORTpass offers a streamlined interface and verification process. Visit **https://portpass.ca** for complete information.

[32] On September 15, 2021, the Government of Alberta announced its "Restrictions Exemption Program" (REP), which came into effect on September 20, 2021.[11] The REP ended February 9, 2022.[12]

[33] PORTpass operated its proof of vaccination app in parallel with the provincial program; that is, PORTpass ceased to operate on or about February 8, 2022, the same date that the REP was removed.

[11] Government of Alberta. "New vaccine requirements and COVID-19 measures in Alberta". September 15, 2021. Retrieved from https://www.alberta.ca/release.cfm?xID=79835371972F5-959C-11E8-8A4B6C2B5B2084EB.
[12] Government of Alberta. "Alberta takes steps to safely return to normal". February 08, 2022. Retrieved from https://www.alberta.ca/release.cfm?xID=8185996876395-A336-5B57-A82D6FEE916E1060.

Jurisdiction

[34] PIPA applies to "organizations" with respect to the collection, use and disclosure of "personal information" by organizations.

[35] Section 1(1)(i)(i) of PIPA defines an "organization" to include "a corporation". At the time this investigation was opened, PORTpass was headquartered in Calgary, Alberta, collected personal information in Alberta, and was an organization as defined in section 1(1)(i)(i).

[36] "Personal information" is defined in section 1(1)(k) of PIPA to mean "information about an identifiable individual".

[37] The complainant in this case reported he was "required to upload my original documents showing proof of vaccination, a copy of my driver's license, and a photo of myself. Although optional I also provided my Alberta Health Care number to the website." This information is about an identifiable individual and is personal information as defined in PIPA.

[38] Section 5(1) of PIPA states: "An organization is responsible for personal information that is in its custody or under its control."

[39] PORTpass collected the complainant's personal information via online submission; the personal information was in PORTpass' custody and/or control. PORTpass is responsible for the personal information.

Methodology

[40] I took the following steps in this investigation:

- Mailed initial letter regarding the complaint to PORTpass and the complainant on October 15, 2021. The letter requested that PORTpass provide evidence by November 15, 2021.
- Reviewed the complaint, including supplementary information (correspondence between the complainant and PORTpass) supplied by the complainant.
- Submitted questions to PORTpass on multiple dates between October 20, 2021 and February 18, 2022. Received responses on October 28, 2021, November 4, 2021, November 15, 2021, and December 6, 2021. Reviewed the responses received.
- Spoke with the PORTpass CEO on September 28, 2021, October 21, 2021, multiple dates in November 2021, and February 18, 2022 to discuss questions and seek responses.
- Conducted open-source research of news media, The Internet Archive ("Wayback Machine" or "WBM"), as well as the PORTpass website (while it was operational).

Issue

[41] I identified the following issue for the investigation:

- Did the Organization protect personal information that is in its custody or under its control by making reasonable security arrangements in compliance with section 34 of PIPA?

Analysis, Findings and Recommendations

Issue: Did the Organization protect personal information that is in its custody or under its control by making reasonable security arrangements in compliance with section 34 of PIPA?

[42] PORTpass reported two privacy incidents to the Commissioner, and a breach notification decision was issued on November 19, 2021. Based on information provided by PORTpass, the two incidents were summarized in the breach notification decision as follows:

- 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.

[43] The breach notification decision confirmed the incidents involved the unauthorized disclosure of personal information in PORTpass' control such that a reasonable person would consider that there exists a real risk of significant harm to individuals as a result of the unauthorized disclosure. The decision required PORTpass to notify affected individuals.

[44] This investigation, however, is concerned with PORTpass' compliance with section 34 of PIPA, which requires an organization to make reasonable security arrangements to protect personal information in its custody or under its control to protect against such risks as unauthorized disclosure. Section 34 of PIPA reads:

> An organization must protect personal information that is in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction.

[45] Reasonable security arrangements include administrative, technical, and physical controls. PORTpass' administrative and technical safeguards are at issue in this investigation, given the nature of the complaint under investigation.

Administrative Controls

[46] Administrative controls include policies, processes and practices that govern an organization's collection, use, disclosure and retention of personal information. Administrative controls also include contracts with third party providers that address privacy and security of personal information.

[47] Section 6(1) of PIPA requires that an organization "develop and follow policies and practices that are reasonable for the organization to meet its obligations under this Act." Further, section 6(3) states: "An organization must make written information about the policies and practices referred to in subsections (1) and (2) available on request."

[48] On November 5, 2021, I wrote to PORTpass with a number of questions related to the breaches. I also requested that PORTpass provide documents that were in effect when the initial breach occurred (on or about September 27, 2021):

> Please provide the following documents for my review.
>
> - Privacy policy,
> - Terms of use,
> - Collection notice(s) and/or consent form(s), presented to users prior to the collection of personal information or registering on the platform,
> - Organizational/internal privacy and security policies in place to safeguard personal information, including:
>
> i. Policies governing the collection, use and disclosure of personal information,
> ii. Data handling and retention policies,
> iii. Breach and incident response policies or practices, and
>
> - An overview of what technical safeguards were in place to safeguard personal information.

[49] PORTpass provided a written response on November 15, 2021. However, the response focused almost entirely on the privacy breaches that had occurred and PORTpass' actions to respond to the breaches.

[50] PORTpass did not provide any documents detailing its organizational privacy and security management programs, policies, or practices implemented to protect personal information before a breach occurs.

[51] Instead, with respect to my request for policies and procedures, PORTpass submitted URLs that linked to then-current versions of its Privacy Policy and Terms of Service (Terms). That is, PORTpass provided the URL for its Privacy Policy that was "Last Revised: October 04, 2021," and the URL for its Terms of Service that was "Last Revised: October 03, 2021." Given the dates on these documents, they could not have been in place in September 2021 when the initial breach occurred; nonetheless, I reviewed these documents and was also able to examine archived/cached versions of them via the WBM.

[52] With respect to "Privacy," the various versions of PORTpass' Terms of Service say:

> Your privacy is important to us and **we are committed to protecting your information in accordance with applicable laws and regulations and consistent with our established policies**. Additionally, the Privacy Policy which is incorporated into these Terms, describes how PP will collect information about you through the App and how we use, disclose, and protect that information. [emphasis added]

[53] The PORTpass Privacy Policy (both September 1 and October 4 versions) included limited statements related to privacy and security of personal information:

> 4. Sharing Your Data
>
> Except in the instances listed below, we will not disclose your personal data to others unless you consent to it, nor will we ever sell your personal data to advertisers. However, we share your personal data in the following ways:
>
> • We may share information with vendors, consultants, and other service providers who need access to such information to carry out work for us. **Their use of personal data will be subject to appropriate confidentiality and security measures (e.g. cloud providers who host our App)**.
>
> ...
>
> 9.1 Security of Your Personal Data.
>
> Security of personal data is important to us. We implement security safeguards designed to protect your personal data. This includes safeguards to protect against anticipated threats or hazards to the security or integrity of the data, and to protect against unauthorized access, acquisition, leak, destruction, alteration, loss, disclosure or destruction. Despite these efforts, we cannot guarantee that your data may not be accessed, disclosed, altered, or destroyed by a breach of any of our physical, technical, or administrative safeguards. Please notify us immediately at support@portpass.ca if you become aware of any security issues relating to our App. [emphasis added]

[54] Despite these statements and my request that PORTpass provide me with "Organizational/internal privacy and security policies in place to safeguard personal information", I did not receive any written policies or documentation of any kind from PORTpass to establish that it had developed and followed policies and practices to protect personal information.

[55] I did not receive any information concerning how PORTpass ensures the privacy and security of personal information when contracting with third-party service providers, such as cloud providers who hosted the app.

[56] Further, while the statements in the Terms of Service and the Privacy Policy refer to "appropriate confidentiality and security measures", "established policies" and "security safeguards designed to protect your personal data", they do not demonstrate that PORTpass had these administrative safeguards in place.

[57] I found no evidence PORTpass implemented reasonable administrative security arrangements to protect personal information from such risks as unauthorized disclosure.

Technical Controls

[58] Technical controls include configuration of access controls, intrusion detection, encryption, and other safeguards that mitigate the risk of loss, unauthorized access or disclosure of personal information.

[59] As described above, I wrote to PORTpass on November 5, 2021 and requested it provide me with, "An overview of what technical safeguards were in place to safeguard personal information."

[60] PORTpass did not provide the requested overview, but instead provided URLs that linked to then-current versions of its Privacy Policy and Terms of Service (Terms). I reviewed these documents to understand the technical safeguards PORTpass had in place to protect personal information, as well as information on PORTpass' website.

[61] The Terms of Service did not include any description of PORTpass' technical safeguards; however, it did include a section controlling the conduct of users:

> YOUR CONDUCT
>
> You agree to comply with all laws, rules, and regulations applicable to your use of the App. In addition, you agree not to:
>
> - upload, transmit, or otherwise make available any information that is known by you to be false, inaccurate, or misleading;
> - take any action that interferes with the proper working oft he App or related services, compromises the security of the App or related services, or otherwise damages the App, related service, or any materials and information available through App;
> - attempt to gain unauthorized access to any portion or feature of App, to any other systems or networks connected to the App, to any of our servers, or to any of the services offered on or through the App, including but not limited to by hacking, password "mining", or any other unauthorized means;
> - probe, scan, or test the vulnerability of the App or any network connected to the App or bypass the authentication measures on the App or any network connected to the App without our prior permission;
> - install any software, file, or code that is not authorized by the user of a computer or mobile device or that assumes control of all or any part of the processing performed by a computer or mobile device without the authorization of the user of the computer or mobile device;
> - interfere with or disrupt the operation of the App or server networks connected to the App, or disobey any requirements, procedures, policies, or regulations of networks connected to the App; or
> - use any automated means to collect information or content from or otherwise access the App, including but not limited to through the use of technical tools known as robots, spiders, or scrapers, without our prior permission.

[62] The Terms of Service also included the following disclaimer:

> DISCLAIMERS
>
> Because you control the extent to which the information collected and used by the App is shared, **PP assumes no liability or responsibility for how your information is used or disclosed once it has been**

> **submitted to and stored on the App**. In addition. PORT pass assumes no liability for any actions taken, including any further use or disclosure of your information, by persons to whom you have provided access to any health passes generated by the App or other information collected or used by the App. This includes but is not limited to actions taken to prevent you from boarding an airline or from entering a country at your destination. **You agree that you will hold PP harmless from and against any and all actions, claims, or damages resulting from any use or misuse of the App, or any use or disclosure of your health records and/or other information stored in or accessed through the App**. [emphasis added]

[63] Similarly, PORTpass' online Privacy Policy (September 1 and October 4 versions) included limited and general statements alluding to technical safeguards implemented to protect personal information:

> 7 . DATA TRANSFER
>
> When you use our App, you may be sending personal data into countries that have different data protection rules than those of your country (applicable to individuals signing up for the PORT pass, whom are not Canadian citizens. **However, as a PP user in Canada, all data is stored with Amazon Canada in Central Canada with Cloudflare security until the users PP account is verified. Once a user is verified, all PP holder data is flushed from the Amazon Canada server in Central (Canada) and no personal data is on file once a user is verified, just a users profile image, name and status in a colour coded/icon manner with the secured and encrypted visible digital seal (VOS) called MapleCode a QR code.** We take appropriate steps to protect your personal data when it is transferred across borders, and **certain laws may require us to implement particular safeguards i**ncluding ensuring there is adequate level of protection for the data transferred.
>
> ...
>
> 9. OTHER IMPORTANT INFORMATION
>
> **9.1 Security of Your Personal Data**. Security of personal data is important to us. We implement security safeguards designed to protect your personal data. This includes safeguards to protect against anticipated threats or hazards to the security or integrity of the data, and to protect against unauthorized access, acquisition, leak, destruction, alteration, loss, disclosure or destruction. Despite these efforts, we cannot guarantee that your data may not be accessed, disclosed, altered, or destroyed by a breach of any of our physical, technical, or administrative safeguards. Please notify us immediately at support@portpass.ca if you become aware of any security issues relating to our App.

[64] The PORTpass website, operational at the start of this investigation, referred to some technical safeguards implemented to protect personal information against risks such as unauthorized disclosure. For example, the website described PORTpass as a...

> ...digital health pass app and system built in Canada that can display various user-controlled health statuses and international or domestic province-to-province travel guidelines about the PORTpass™ holder **in the most secure way through AI integration and Blockchain technology**.[13] [emphasis added]

[65] The website also said PORTpass is "fully secured blockchain enabled and encrypted" and, "Verifiers will not have access to any user information, only what the user would like to show

[13] PORTpass Inc. "Our Solutions", n.d. Retrieved from https://web.archive.org/web/202109290101312/https://portpass.ca/solutions/ on March 11, 2022.

you through their … mobile app."[14] None of the submissions I received from PORTpass contained information concerning use of blockchain and AI technology.

[66] Overall, I did not receive any evidence to demonstrate that PORTpass implemented reasonable technical security arrangements to protect personal information from such risks as unauthorized disclosure.

Updated Breach Report

[67] PORTpass' updated breach report, submitted to the OIPC on October 11, 2021, described steps taken to reduce the risk of similar events occurring in the future. The report described steps taken after the breaches occurred, and not security arrangements that were implemented to protect personal information against risks such as unauthorized disclosure:

> On [S]eptember 28, 2021 PORTpass notified the Cybercrime unit at the Calgary Police Service, we got on that day an email for OPPC and the Alberta Privacy commissioner.
>
> We have also been in conversation with Gov of Alberta and Alberta Health in finding ways to work together, get help and advice as Stakeholders for the public safety.
>
> Our team has hired a cybersecurity firm to help us with each step to implement the best programs and strategies into place to continue to keep our user data secured.
>
> We have also started working with auditors for SOC 2 Type 2 Compliance and HIPAA to ensure the safety of the users of the PORTpass app for IOS and Android Devices.
>
> The team at PORTpass also added some new technologies that are used across our nation in hospitals and fintech institutions to bring the utmost security and peace as we grow through these fast paced and challenging times with confidence.
>
> Adding safeguards such as a Bug bounty program to encourage ethical testing and responsible disclosure Improved authentication on every page to ensure that only humans access pages they are authorized to access.
>
> Enhanced monitoring process
> Security consultation during the design, implementation, and change processes
> Ongoing vulnerability scanning and active manual penetration testing
> Minimize collected data
> Enhanced web application firewall rules
> Additional redundancy to handle peak loads
> Additional security controls
>
> We are also doing our SOC 2 Type 2 Audit soon as we have been compiling our data and will be being proactive with a PIA by also bringing on a custodian as a health director.
>
> We have also created crisis management measures and various other elements that we were learning in the process that we have now implemented to get matters resolved and out to the affected individuals immediately. Including, now knowing who to contact -- for any questions/concerns/thoughts.

[14] *Ibid*.

[68] PORTpass made numerous references to a third-party "cybersecurity firm" it retained to assist it in responding to the breaches. On January 5, 2022, I asked to review the third party cybersecurity report; I also repeated my request for documents regarding PORTpass' privacy and security programs. My emails were rejected by PORTpass' mail server; the email addresses I used to communicate with PORTpass no longer existed. On January 6, 2022, I attempted to call PORTpass in order to obtain new contact information. No one answered and my call was not returned.

[69] As previously described, on February 18, 2022, I received a response to an email request for information, and had a telephone conversation with PORTpass' CEO. The CEO advised that PORTpass was no longer operating (in tandem with the Government of Alberta ending the Restrictions Exemption Program) and had "removed the database" containing personal information. PORTpass committed to providing further clarification on February 22, 2022.

[70] PORTpass did not report back on February 22. That same day, the OIPC confirmed via CORES search that PORTpass had legally dissolved on or about February 8, 2022.

Conclusion

[71] Given the above, I find PORTpass did not protect personal information in its custody or under its control by making reasonable security arrangements against such risks as unauthorized access, collection, use, disclosure, copying, modification, disposal or destruction, in contravention of section 34 of PIPA.

[72] As PORTpass is now dissolved, there is no longer an "organization" as defined in PIPA to whom the Commissioner can make recommendations, or against whom an order compelling compliance can be issued.

[73] With respect to the individual who complained to the OIPC, on December 6, 2021, PORTpass said that "the issue had been resolved" and that "the third-party cyber security audit" confirmed the complainant "was not on the list nor was his email address." Further, I understand from the complainant that the Calgary Police Service (CPS) also conducted an investigation into the PORTpass incidents. CBC News reported the CPS investigation concluded in October 2021, and found no evidence of "criminal attacks or data breaches."

[74] This was a timely investigation, occurring at the intersection of technology developed in response to a public health emergency. Despite the pressures of the pandemic, organizations remain accountable for safeguarding personal information in their custody or their control. I remind organizations that they ought to be able to demonstrate that reasonable safeguards are in place to protect privacy, especially when collecting and using sensitive identity and medical information.

[75] I wish to thank the complainants for coming forward with their concerns.

Eric Cheung
Senior Information and Privacy Manager