AMERICAN CIVIL LIBERTIES UNION
Rhode Island

128 Dorrance Street, Suite 400
Providence, RI 02903
Phone: (401) 831-7171
Fax: (401) 831-7175
www.riaclu.org
info@riaclu.org

December 28, 2021

VIA MAIL AND EMAIL

Scott Avedisian, CEO
Rhode Island Public Transit Authority
705 Elmwood Avenue
Providence, RI 02907

Dear Mr. Avedisian:

I am writing on a matter of great urgency, and that is to seek answers to questions that have been raised by a security breach at RIPTA that has led to the unauthorized release of personal health care information of thousands of individuals who have no relationship with RIPTA at all. It is essential that RIPTA provide answers to the public as to why it had this private information in the first place and why it has provided misleading information about this security breach to the public.

Specifically, in the past 24 hours, our office has received complaints from individuals who received letters from your agency advising them that their personal data, including personal health care information, was accessed in a security breach of RIPTA's computer systems. According to the letter, the information that was stolen included the person's "name, Social Security number, and one or more of the following: address, date of birth, Medicare identification number and qualification information, health plan member identification number and claims information."

Needless to say, they found this breach of their personal information quite disturbing and are concerned about its potential impact on their medical privacy and on their potential victimization from identity thieves. They are also deeply concerned about the length of time it took for them to be notified of this security breach. Again, according to the letter, the breach was identified on August 5th, but it was purportedly not until October 28th – over two and half months later – that RIPTA identified the individuals whose private information had been hacked, and it then took *almost two more months* to notify those individuals.

But worst – and most inexplicable – of all, the people who have contacted us are even more deeply distressed by the fact that RIPTA somehow had any of their personal information – much less their personal *health care* information – in the first place, as *they have no connection at all with your agency*.

The information that has been provided publicly by RIPTA about this security breach is, in many ways, significantly and materially different from the information RIPTA has provided the affected individuals about it. According to the public notice posted on your website on or about December 21st about this security incident, the breach involved the "personal information of *our* health plan beneficiaries." The public notice further states that a review of the files that had been "exfiltrated" by the hackers identified them as "files pertaining to *RIPTA's* health plan." (emphasis added) However, based on the complaints we have received, this is extremely misleading and seriously downplays the extensive nature of the breach. Most importantly, it ignores, and fails to address, a host of questions regarding how the information that was hacked was in RIPTA's hands in the first place.

Contrary to your agency's statement that the breach involved RIPTA's health care beneficiaries, all the complaints we have received have come from people *who have never been RIPTA employees and, in some instances, have never even ridden a RIPTA bus*. The only connection that they all seem to have is that they are, or were, state employees. Nothing in RIPTA's notice or letter explains why the personal health care information of non-RIPTA employees was in its computer system in the first place.

In addition, according to the information posted on the U.S. Department of Health and Human Services website that tallies breaches of personal health care information – information presumably provided by RIPTA – there were 5,015 people affected by the breach. However, the letter that individuals have received indicates that the incident involves 17,378 individuals in Rhode Island – a more than threefold difference.

Under the circumstances, it is essential that RIPTA provide to the public and to the affected individuals some critical clarification and information about this incident. Specifically:

1. Please explain why it took more than 2 ½ months for RIPTA to identify the people whose names and information were hacked, and why it then took two more months to notify them.

2. Please explain how and why data on RIPTA's hacked server included personal information, including medical information, of individuals who had no contact with RIPTA.

3. Assuming that the information was somehow inadvertently provided to RIPTA by a health care provider, how and why did RIPTA not realize this error, notify the provider and immediately delete all this personal information?

4. Please explain why the information provided the U.S. Department of HHS refers to 5,015 people affected, but the letter sent to affected individuals indicates that 17,738 people were affected.

In this electronic age, we realize that personal data is a precious commodity and one zealously sought after by bad actors. We also recognize the challenges faced in keeping electronic information secure from malicious hackers. But that is what makes all the more alarming the specifics of this incident: the time it took for affected individuals to be notified, the misleading information provided the public about it, and, most critically of all, RIPTA's possession and storage of personal health care information that it clearly had no business having in the first place.

I look forward to hearing back from you about this at the earliest possible opportunity, and request that you also provide answers to these questions to all the individuals who have received individual notice in the past few days of the breach involving their personal information.

Sincerely,

Steven Brown
Executive Director

cc: The Hon. Peter Neronha, Attorney General
Patrick Tigue, Health Insurance Commissioner

RHODE ISLAND PUBLIC TRANSIT AUTHORITY

Steven A. Colantuono
Chief Legal Counsel
401-784-9500, ext. 1139
scolantuono@ripta.com

January 5, 2022

Mr. Steven Brown
Executive Director
American Civil Liberties Union
128 Dorrance Street, Suite 400
Providence, RI 02903

Dear Mr. Brown:

We write in response to your December 28, 2021 letter regarding RIPTA's data security incident. As you are aware, on August 5, 2021, we identified unauthorized access to RIPTA's computer systems. We immediately secured the systems involved and began an investigation. The investigation determined that an unauthorized party exfiltrated files from RIPTA's systems between August 3, 2021 and August 5, 2021. We conducted a careful review of these files and, on October 28, 2021, determined they contained personally identifiable information and personal health information.

Since learning of this incident, RIPTA worked diligently to identify all individuals whose information was contained in the files that were accessed or exfiltrated by the unauthorized party. After the analysis was complete, RIPTA searched its records and identified address information for the individuals being notified. This process was time and labor-intensive, but RIPTA wanted to be certain about what information was involved and to whom it pertained.

RIPTA uses the same state organized health insurance plan as other non-RIPTA state agencies. RIPTA's prior healthcare provider made a report available to RIPTA that included information for individuals under the state organized plan, which included non-RIPTA employee information. These files were involved in the data security incident, which is why RIPTA notified non-RIPTA employees. RIPTA no longer uses this healthcare provider and is in the process of isolating and removing all non-RIPTA employee information from its systems.

The total number of individuals whose personal health information was affected by the incident pursuant to HIPAA is 5,015. Given the nature of the information involved, there were also individuals whose personal information was affected. The access to this information did not require notice to individuals pursuant to HIPAA. Rather, RIPTA notified these individuals pursuant to state law. In total,

17,378 Rhode Island residents were notified. Because of the different legal notification obligations under HIPAA and state law the number of individuals reported to OCR differs from the number of Rhode Island residents listed as affected on the notice letters to individuals.

Should you have any additional questions, please call our dedicated call center at 855-604-1668 Monday through Friday from 9AM – 9PM EST, except holidays.

Sincerely,

Steven Colantuono (rr)

Steven A. Colantuono
Chief Legal Counsel

AMERICAN CIVIL LIBERTIES UNION
Rhode Island

128 Dorrance Street, Suite 400
Providence, RI 02903
Phone: (401) 831-7171
Fax: (401) 831-7175
www.riaclu.org
info@riaclu.org

February 9, 2022

VIA MAIL AND EMAIL

Scott Avedisian, CEO
Rhode Island Public Transit Authority
705 Elmwood Avenue
Providence, RI 02907

Dear Mr. Avedisian:

I am writing to follow up on my December 28th letter to you and the January 31st hearing held by the Senate Oversight Committee regarding the RIPTA security breach matter. I appreciate the response to my letter that I received from Mr. Colantuono and the testimony that was provided by you and other RIPTA representatives at the hearing. As I mentioned in my testimony, however, I believe that the information provided at the hearing raised as many questions as it answered. I am therefore hoping you can provide some additional insights and clarify some of the information given.

I apologize for the lengthy list of questions, but I think it demonstrates the lack of clarity that remains as to exactly what happened.

1. Your agency reported to the federal Office of Health and Human Services potential breaches of medical information of 5,015 people. You also stated at the hearing that, at any given time, RIPTA has about 800 employees. This raises many questions:

a. Were all of the 5,015 individuals whose medical information was potentially breached current or former RIPTA employees, or does it also include dependents of RIPTA employees?

b. Does the 5,015 number represent the entire universe of current and former employees of RIPTA who were in the database, or is the number limited to a subset of RIPTA employees whose information was in the hacked database(s)?

c. Does the 5,015 number include any individuals – whether employees, dependents, or retirees – of other, non-RIPTA state departments or quasi-public agencies?

2. Did the 5,015 people receive a letter different from the December 21st letter we have seen, which merely indicates that the recipient *may* have had their medical information disclosed? If they received the same letter, is there a reason RIPTA has not been more explicit with them about the breach of medical data? If they received a different letter, could you send us a sample?

3. Does the 5,015 number include any of the 5,000 or so non-residents of the state who were publicly reported for the first time at the legislative hearing as having their information breached?

4. Have the non-resident former state employees or their dependents received a letter from RIPTA about the data breach? If so, on what date did the letter get sent to these individuals and is it the same as the letter that was sent out on December 21st to others?

5. RIPTA's December 21st letter advises individuals that the exfiltrated files included "*one or more* of the following: address, date of birth, Medicare identification number and qualification information, health plan member identification number and claims information." (emphasis added). Can you explain why you're uncertain exactly what pieces of information from the files were exfiltrated?

6. Is it the case that other individuals beyond the reported 5,015 employees may have also had their medical information breached, but that RIPTA concluded it did not need to report those numbers to HHS because they involved non-RIPTA employees?

a. If so, can you explain why you believe you did not have an obligation to report those breaches as well?

b. If so, can you identify the state departments or quasi-public agencies at which they are or were employed?

c. If so, is it your belief that all these individuals may have also had their medical information breached, and if not, how many had only non-medical personally identifiable information breached?

7. At the hearing, you described the files you have seen as containing numerous blank spaces ("filtered" spaces) between the names and other identifying information of RIPTA employees. You indicated that you didn't know if it was possible for somebody to "unfilter" those files. If that is so, how did RIPTA determine the names of the 17,000+ non-RIPTA employees whose information was accessed?

8. To the best of your knowledge, was RIPTA's access to the United Healthcare portal and its ability to download information that included other state employees any different than the way any other state agency would receive the information for auditing purposes? Had RIPTA ever requested any special type of access that might account for its receipt of non-RIPTA information?

I look forward to any additional insights that RIPTA can share on these matters. As you can tell by these questions, much remains to be learned about how this incident occurred and how to prevent it from happening again. Thank you.

Sincerely,

Steven Brown
Executive Director

cc: Steven Colantuono
The Hon. Louis DiPalma
Bijay Kumar, Division of Information Technology