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

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

VIA MAIL AND EMAIL

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