STATE OF RHODE ISLAND
DEPARTMENT OF
ADMINISTRATION

Director's Office

One Capitol Hill | Providence, RI 02908 | 401-222-2280
James E. Thorsen, Director

December 30, 2021

Dear colleagues,

Last week, I shared with you that the Rhode Island Public Transit Authority (RIPTA, a quasi-public agency) informed the State that it was the target of a security incident that involved the disclosure of information of participants of the State's health plans. While this incident did not involve the State's computer network or servers and RIPTA does not share servers or networks with the State, the Department of Administration (DOA) has been working with RIPTA to determine how it received the personal and health information of individuals who are not RIPTA employees

By way of background, on Thursday, August 5, 2021, RIPTA identified a security incident and immediately began an investigation. A careful review and forensic analysis were conducted, and it was discovered that among the affected files were those pertaining to the State's health plan billing. State employee data was incorrectly shared with RIPTA by an external third party who had responsibility for administering the State's employee health benefits program. The files were illegally obtained from RIPTA's server by an unauthorized third party.

The files reportedly contained plan member names, Social Security numbers, addresses, dates of birth, Medicare identification numbers and qualification information, health plan member identification numbers, claim amounts, and dates of service for which claims were filed. We are currently seeking a copy of the files to confirm the data elements.

On Monday, December 20, 2021, RIPTA informed DOA that the incident involved State employee information and stated that letters to affected employees were to be mailed that week. On Wednesday, December 22, 2021, I sent my initial communication to you.

Since that time, we have been informed that the subject period of the data files extends to a currently undetermined point in early 2020 – not merely the 2013-2015 period previously stated. However, it is our understanding that RIPTA sent informative letters to all identified, impacted health plan participants.

In terms of our own activity, we continue to interact with RIPTA personnel to better understand this complex situation; the Office of Employee Benefits and Division of Information Technology teams have addressed data security concerns with our current third-party health plan administrator; the Division of Information Technology team continues to monitor the State's systems and the data it holds; and the Division of Human Resources is providing the best information that we have to concerned individuals calling the Division. Our teams remain hard at work to gain a full understanding of what happened, and I will share additional information once we do. In the coming days, an FAQ document will be posted to the Division of Human Resources' website.

In the meantime, all affected employees and other plan participants should avail themselves of the resources provided by RIPTA, including a complimentary membership to identity monitoring services

through Equifax. And you should take the steps suggested in the RIPTA letter to protect yourself not only because of this breach, but because of the identity threats we all face every day.

RIPTA has established a dedicated call center at 855-604-1668 that is available Monday through Friday (except holidays) from 9 a.m. to 9 p.m., to answer questions.

Sincerely,

James E. Thorsen
Director of Administration