FAQs on Security Incident Involving Employee Information

1. What was the data security incident that occurred at RIPTA?

On Thursday, August 5, 2021, RIPTA identified a data security incident and immediately began an investigation. In connection with that investigation, RIPTA discovered that an unauthorized party accessed or exfiltrated certain files from RIPTA's systems between August 3, 2021 and August 5, 2021. A careful review and forensic analysis were conducted, and in late October it was discovered that among the affected files were those pertaining to the State's health plan billing. The affected 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.

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.

2. When did the data security incident happen?

The investigation determined that an unauthorized party accessed or exfiltrated certain files from RIPTA's systems between August 3, 2021 and August 5, 2021.

3. What personal information of mine was involved?

The affected 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 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.

RIPTA only mailed letters to the individuals whose information was potentially involved in this incident. If you have not or do not receive a letter, your information was not involved in the incident. If you have any questions, please contact RIPTA's dedicated call center at 855-604-1668.

4. Why does RIPTA have my information?

RIPTA participates in the State's organized health insurance plan. State employee data was incorrectly shared with RIPTA by the prior healthcare provider. RIPTA is taking all necessary steps to remove all files containing State employee information, and the State is working closely with all parties involved to ensure that this type of access to State sensitive data is prevented in the future.

5. I left state service and moved. How did RIPTA obtain my current address?

Through a location search for the most current address available.

6. Who is the unauthorized party who accessed or infiltrated RIPTA's files?

RIPTA does not know who is responsible for this incident. State and federal law enforcement authorities have been notified of the data security incident and are investigating.

7. Why was I notified?

If you received a notification letter, it is because your information was contained in a file on RIPTA's computer systems that was accessed or exfiltrated by an unauthorized party. There are State laws that require you to be notified in writing of incidents involving your personal information.

8. What can I do/What should I do now?

We encourage you to actively monitor for the possibility of fraud and identity theft by reviewing your credit report and financial statements for any unauthorized activity. If you notice any unauthorized activity, you should immediately notify the relevant financial institution or credit bureau reporting the activity. In addition, the notification letter RIPTA sent you provides additional steps that you can take to protect your information. The letter also includes instructions for enrollment in a complimentary credit monitoring and identity theft protection service.

9. How many individuals were affected?

In accordance with the letters sent by RIPTA, the incident involves 17,378 individuals. RIPTA provided notice to the individuals whose personal information was contained in files on RIPTA's computer systems that was accessed or exfiltrated by an unauthorized party.

10. Could there potentially be more individuals?

RIPTA's investigation of this incident is complete. RIPTA sent notification letters to everyone whose personal information was accessed or exfiltrated by an unauthorized party.

11. Why did you wait until now to notify me?

On Monday, December 20, 2021, RIPTA informed the Department of Administration that the incident involved State employee information and stated that letters to affected employees were to be mailed that week. Since that time, the Department has continued 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 and protect 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.

12. How could something like this have happened?

All organizations face cybersecurity risks, and RIPTA had security measures in place to help protect against those risks. To strengthen its information security processes, RIPTA is taking steps to enhance its existing security protocols and re-educate employees.

13. What has the State done to keep this from happening again?

In an effort to prevent this from happening at the State, the Division of Information Technology has deployed an in-depth cybersecurity strategy across the enterprise to tackle this challenge from multiple angles, which continues to be improved upon. This includes:

1) *Protect the network edge with intrusion detection and prevention, and firewalls.* The Division (through automation) looks for known malware signatures and IPs and blocks them at the network edge to prevent bad actors from gaining access to the network and systems.
2) *User awareness training.* The Division teaches users how to spot and report the phishing emails that will install malware on devices.
3) *Email sanitization.* The Division (through automation) scans and strips emails of suspicious attachments and content.
4) *Vulnerability scanning and patching.* Every week, the Division scans all connected devices for known vulnerabilities to then patch them so they cannot be exploited if malware were to be introduced. The Division also works to actively lifecycle end of life/end of support IT hardware and software.
5) *Active device monitoring.* The Division actively monitors all endpoints with a cloud-based security continuous monitoring tool that monitors and reports upon all state devices for malicious activity.
6) *Data encryption.* The Division encrypts all sensitive data at rest.

In addition, the Office of Employee Benefits and Division of Information Technology teams have addressed data security concerns with our current third-party health plan administrator to ensure that there is no inappropriate access to or release of data.

14. Was my Social Security number exposed?

Your Social Security number was included in the files that were accessed and exfiltrated by an unauthorized party. We encourage you to actively monitor for the possibility of fraud and identity theft by reviewing your credit report and financial statements for any unauthorized activity. If you notice any unauthorized activity, you should immediately notify the relevant financial institution or credit bureau reporting the activity. In addition, the notification letter that RIPTA sent you provides additional steps that you can take to protect your information and instructions for enrollment in a complimentary credit monitoring and identity theft protection service.

15. Does this mean I am the victim of identity theft?

No. However, RIPTA was required to notify you about this incident so you may take the appropriate steps to protect your information. We encourage you to actively monitor for the possibility of fraud and identity theft by reviewing your credit report and financial statements for any unauthorized activity. If you notice any unauthorized activity, you should immediately notify the relevant financial institution or credit bureau reporting the activity. In addition, the notification letter RIPTA sent provides additional steps that you can take to protect yourself. The notification also includes instructions for enrollment in a complimentary credit monitoring and identity theft protection service.

16. What if I have out-of-pocket expenses related to this issue?

You should review your credit reports and account statements for any unauthorized activity regularly and report any unauthorized activity to the appropriate financial institution or the credit bureau reporting the activity. In addition, the notification letter that RIPTA sent provides additional steps that you can take to protect yourself. The notification also includes instructions for enrollment in a complimentary credit monitoring and identity theft protection service.

17. How will I know if my information is used by someone else?

Again, we encourage you to actively monitor for the possibility of fraud and identity theft by reviewing your credit report and financial statements for any unauthorized activity. If you notice any unauthorized activity, you should immediately notify the relevant financial institution or credit bureau reporting the activity. In addition, the notification RIPTA sent provides additional steps that you can take to protect yourself. The notification also includes instructions for enrollment in a complimentary credit monitoring and identity theft protection service.

18. Now that the incident is resolved, could I still experience fraud?

Even though RIPTA has resolved this incident, you are encouraged to actively monitor for the possibility of fraud and identity theft by reviewing your credit reports and account statements for any unauthorized activity regularly and report any unauthorized activity to the appropriate financial institution or credit bureau reporting the activity. In addition, the notification RIPTA sent provides additional steps that you can take to protect yourself. The notification also includes instructions for enrollment in a complimentary credit monitoring and identity theft protection service.

19. Do I need to change my Social Security number? How is that done?

The Social Security Administration does not routinely assign different Social Security numbers unless specific requirements are met. More information regarding requesting a different Social Security number can be found at the Social Security Administration's website at www.ssa.gov.

Also, if you think someone is using your Social Security number, you should immediately contact the Federal Trade Commission (*Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.idtheft.gov,TTY 1-866-653-4261*) and/or the Attorney General in your state. You should also contact your local law enforcement authorities and file a police report. Also, contact Experian for Identity Restoration assistance which is available under the services being offered.

20. I believe I have experienced fraud/identity theft. What do I do?

The first step is to alert the institution where you believe the fraud occurred, or where the fraudulent account was opened. You should contact the Federal Trade Commission and the Office of the Attorney General in your state. You can obtain information from these sources about steps an individual can take to avoid identity theft as well as information about fraud alerts and security freezes. You should also contact your local law enforcement authorities and file a police report. Obtain a copy of the police report in case you are asked to provide copies to creditors to correct your records. Contact information for the Federal Trade Commission is as follows: *Federal Trade Commission, Consumer Response Center, 600 Pennsylvania Avenue NW, Washington, DC 20580, 1-877-IDTHEFT (438-4338), www.ftc.e.ov/idtheft.*

21. Will someone steal my identity?

If you ever believe you have been the victim of identity theft or have reason to believe your information is being misused, we urge you to immediately contact the police and file a police report. Obtain a copy of the police report as you may need to provide copies of the report to creditors to clear up your records. You may also contact the Federal Trade Commission and the Office of the Attorney General in your state. You may obtain a copy of your credit report, free of charge, directly from each of the three

nationwide credit reporting companies. To order your annual free report please visit www.annualcreditreport.com, call toll free at 1-877-322-8228, or directly contact the three nationwide credit reporting companies:

Experian, P.O. Box 2002 Allen, TX 75013 www.experian.com or 1-888-397-3742

Trans Union, P.O. Box 2000 Chester, PA 19016 www.transunion.com or 1-800-916-8800

Equifax, P.O. Box 740241 Atlanta, GA 30374 www.equifax.com or 1-800-685-1111

You may also take advantage of the complimentary identity restoration service offered in the letter you received from RIPTA.

22. Is RIPTA offering credit monitoring?

Yes, to individuals whose Social Security Number was potentially involved. The State encourages you to actively monitor for the possibility of fraud and identity theft by reviewing your credit report and financial statements for any unauthorized activity. If you notice any unauthorized activity, you should immediately notify the relevant financial institute or credit bureau reporting the activity. In addition, the notification RIPTA sent provides additional steps that you can take to protect yourself, including instructions for enrollment in a complimentary credit monitoring and identity theft protection service.

23. Can my family member also receive free credit monitoring services?

If your family member's information was potentially involved, he or she will be sent a letter, which provides further steps that your family member can take to protect their information.

24. How does someone obtain a free copy of his or her credit report?

You may obtain a copy of your credit report, free of charge, directly from each of the three nationwide credit reporting companies. To order your annual free report please visit www.annualcreditreport.com, call toll free at 1-877-322-8228, or directly contact the three nationwide credit reporting companies:

Experian, P.O. Box 2002 Allen, TX 75013 www.experian.com or 1-888-397-3742

Trans Union, P.O. Box 2000 Chester, PA 19016 www.transunion.com or 1-800-916-8800

Equifax, P.O. Box 740241 Atlanta, GA 30374 www.equifax.com or 1-800-685-1111

25. I use/am buying another credit monitoring/identity protection product. I want RIPTA to reimburse me. Who do I speak with?

RIPTA is not compensating individuals for identity theft protection services purchased outside of the complimentary credit monitoring and identity theft protection services that have been offered to eligible individuals. Enrollment instructions are included in the notification letters sent to those individuals.

26. Will enrolling in credit monitoring affect my credit?

No. Enrollment in the identity monitoring services, provided at no cost to you, will not affect your credit.

27. Should I sign up for the credit monitoring services?

While it is your choice, we encourage you to sign up for the credit monitoring services. The details of the free services RIPTA is offering are contained in the letter and on the websites listed in the letter.

28. Will I be automatically charged after the complimentary credit and identity monitoring service expires?

No, you will not be charged automatically after your complimentary identity monitoring services expire. You do not need to provide any payment information to enroll in the services.

29. Is this notification a solicitation to purchase identity monitoring products?

No, the notification you received is not an attempt to get you to purchase any services. RIPTA notified you about this situation and is offering complimentary identity monitoring services through Equifax.

30. Should I freeze my credit? What is a credit or security freeze?

That is up to you. You have the right to put a "security freeze," also known as a credit freeze, free of charge, so that no new credit can be opened in your name without the use of a PIN number that is issued to you when you initiate a freeze. A security freeze is designed to prevent credit, loans, and services from being approved in your name without your consent. If you place a security freeze, potential creditors and other third parties will not be able to get access to your credit report unless you temporarily lift the freeze. Therefore, using a security freeze may delay your ability to obtain credit.

There is no fee to place or lift a security freeze. Unlike a fraud alert, you must separately place a security freeze on your credit file at each credit reporting company. For information and instructions to place a security freeze, contact each of the credit reporting agencies at the addresses below:

Experian Security Freeze, PO Box 9554, Allen, TX 75013, www.experian.com

Trans Union Security Freeze, PO Box 2000, Chester, PA 19016, www.transunion.com

Equifax Security Freeze, PO Box 105788, Atlanta, GA 30348, www.equifax.com

31. Should I request a fraud alert from the credit reporting agencies? What is a fraud alert?

That is up to you. There are two types of fraud alerts you can place on your credit report to put your creditors on notice that you may be a victim of fraud – an initial alert and an extended alert. You may ask that an initial fraud alert be placed on your credit report if you suspect you have or are about to be, a victim of identity theft. An initial fraud alert stays on your credit report for at least one year. You may have an extended alert placed on your credit report if you have already been a victim of identity theft with the appropriate documentary proof. An extended fraud alert stays on your credit report for seven years. You can place a fraud alert on your credit report by calling the toll-free fraud number of any of the three national credit reporting agencies as follows:

Experian: 1-888-397-3742, htlps://www.experian.com/fraud/center.html

Trans Union: 1-800-680-7289, https://www.transunion.com/fraud-victim-resource/place-fraud-alert

Equifax: 1-888-766-0008, https://www.alerts.equifax.com

32. My Activation Code for the complimentary identity monitoring services is not working, what do I do?

RIPTA has confirmed that these codes are valid and active. Please contact Equifax Customer Service at the number provided in your letter. They will be able to assist you with any issues you have with your activation code. They will also be able to enroll you over the phone.

33. Any other questions regarding the incident:

Please contact RIPTA's call center at 855-604-1668, Monday through Friday, from 9AM - 9PM EST, except holidays.