Frequently Asked Questions

Questions & Responses:

1. **What Happened?**

   On the morning of March 16, 2024, City of Pensacola IT members detected and stopped a ransomware attack in which an unauthorized third party accessed some of our systems. Local, state and federal law enforcement agencies are investigating this incident.

2. **Why does the City of Pensacola, Pensacola Energy or Pensacola Sanitation have my information?**

   Employees: If you received a letter, it is because you are a current or former employee of the City of Pensacola.

   Customers: I you received a letter, it is because you are a current or former customer of Pensacola Energy and/or Pensacola Sanitation.

3. **When did the City of Pensacola find out about this breach?**

   The security incident was discovered on March 16, 2024. However, on April 2, 2024, the City of Pensacola completed a comprehensive internal review of the data impacted in this incident and determined that customer and employee data was likely impacted. Therefore, the City of Pensacola has opted to notify all employees and customers out of an abundance of caution.

4. **I received a letter in the mail. Is this fraudulent, a scam, or a real incident?**

   Federal and state laws require that we notify by mail any person whose information was compromised. We can assure you that this incident did occur, and thus, we are offering the support identified within the notification letter. We would encourage you to take advantage of the identity monitoring services provided and call us at the number noted within the letter if you have further questions or concerns.

5. **Why didn't you just call me?**

State and Federal laws require written notification. Also, we wanted to be sure you knew this was a legitimate notice and that the affected people received the notice.

6. Why did you wait so long to notify me?

We understand your concerns. We moved as quickly as we reasonably could. It took us time to determine what information was compromised and who was affected. Although we realized on March 16, 2024, that an incident took place, we were not able to determine the extent of the incident until we completed a comprehensive investigation with the help of forensic experts. Once this investigation was completed, we undertook an exhaustive review of data impacted in this incident, which takes time to identify impacted individuals properly and accurately. Through our review, we determined those individuals who required notification. We then went through a due diligence to identify updated address information for all potentially impacted individuals before sending letters.

7. What kind of data was compromised?

Although we have no evidence that your information has been specifically misused, it is possible that certain personal information could have been exposed to the unauthorized party. Please reference your letter for the types of information potentially at risk.

8. Why was the city in possession of my Social Security number?

Employees: The City of Pensacola maintains your Social Security number for administrative, payroll and human resources purposes for employees.

Customers: Pensacola Energy and/or Pensacola Sanitation maintains your Social Security number for administrative and/or billing purposes.

9. How many people were affected by the data breach?

We do not have this information, but identifiable individuals whose information was potentially compromised have been sent notification letters.

10. Who is TransUnion? I thought my information was held by the City of Pensacola.

The City of Pensacola engaged TransUnion to provide you with services following the incident. TransUnion is a legitimate company and will help enroll those eligible for credit monitoring.

Moving Forward

11. Has the data involved in this incident been misused?

Since we discovered the incident (from March 16th to the present), the City of Pensacola has not received any reports of related identity theft.

12. What is the City of Pensacola doing to make sure this does not ever happen again?

We are reviewing all our current security protocols and adding additional security measures as needed to prevent this from happening again. IT professionals conducted a thorough investigation and provided recommendations for security enhancement.

Identity Theft Concerns

13. I am concerned about identity theft - what can I do?

There are a variety of steps you can take, many of which were detailed in the letter you received. These include placing a fraud alert with the credit bureaus, reviewing your financial statements, and signing up for credit monitoring.

14. Why do I have to provide TransUnion with my social security number?

Your Social Security number is your unique identifier with the credit bureaus, and TransUnion needs this information to provide you with credit monitoring services. We have not provided TransUnion with those numbers since they don't need them unless you choose to enroll in the free credit monitoring.

15. What will happen if I find out my identity has been stolen?

In the unlikely event that your information is misused, a TransUnion personal advocate will work with you from the first call you make to report the problem until

the crisis is resolved. TransUnion will notify the appropriate agencies, businesses and institutions and create a comprehensive case file.