City of Franklin
Frequently Asked Questions

1. **What happened?**

On or about August 15, 2024, the City of Franklin ("Franklin") became alerted to a cybersecurity incident. An unauthorized third party attempted to infiltrate Franklin's network. Upon detecting the incident, Franklin moved quickly to secure the network and launched an investigation to determine the scope and extent of any potential unauthorized access of our systems. The investigation was conducted with the help of independent IT and forensic investigators.

2. **When did the City of Franklin ("Franklin") learn of this incident?**

Franklin became alerted to the incident on or about August 15, 2024. However, the investigation that identified the personal information that was impacted recently concluded on May 19, 2025.

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

Federal and state laws require that we notify you by mail. 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.

4. **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.

5. **Why didn't you contact me before? / Why did it take this long to notify me?**

Upon detecting the incident, Franklin moved quickly to secure its network and launched an investigation to determine the scope and extent of any potential unauthorized access of our systems with the assistance of external forensic experts. The investigation that identified the personal information that was impacted recently concluded on May 19, 2025.

Franklin then worked quickly to provide notification to potentially impacted individuals. It took time for Franklin to conduct the investigation into the scope of impact, prepare notification letters, perform a NCOA search to secure updated addresses for each individual, and engage a vendor to send notification letters to potentially impacted individuals.

6. **What kind of data was compromised?**

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

7. Has my information been misused?

Franklin has not received any reports of related identity theft since the date the incident was discovered (August 15, 2024, to present).

8. Does Franklin know who is responsible for this?

No, the identity of the party responsible for this incident is still being investigated.

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

We do not have this information, but every individual potentially compromised has received a similar letter.

10. Is my spouse/family member/friend affected?

Each impacted person will, or should have received a letter from Franklin. Unless he/she/they has received a letter, he/she/they is not affected by this incident.

11. How is someone who is deceased receiving a letter?

The unauthorized person had access to a server that had information on that potentially went back to the 1960's. All those who may have been impacted by this incident were notified. This may have included people who are deceased, have moved, or changed their name. Mailing addresses were determined by the Transunion Federal Bureau, which may or may not be currently accurate.

12. What is Franklin doing to make sure this does not ever happen again?

The security and privacy of personal data remains one of Franklin's highest priorities. In response to this incident, Franklin has taken steps to prevent a similar incident from occurring in the future by implementing additional safeguards and enhanced security measures.

13. Who is Transunion? I thought my information was held by Franklin.

Transunion has been hired by Franklin to provide you with services following the incident.

14. Who is Cyberscout?

You have dialed the toll-free assistance line set up by Franklin to provide individuals with additional information about the incident. We are not part of Franklin and do not have access to your personal information. We have been engaged by Franklin to provide you with basic information regarding the event and access to resources to assist you with enrolling in identity protection services and preventing identity theft and fraud. If you would like to speak directly with Franklin, please provide your name and contact information and someone with Franklin will contact you.

15. What can I do to protect against identity theft or fraud?

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.

16. I am not satisfied that you are doing enough to protect me - what else can you do to help? I will be contacting my attorney or filing a lawsuit.

We understand your concerns. Please contact Transunion at 1-833-367-5713 and allow them to take your name and number and they will have Franklin management give you a call back directly soon to discuss this with you further.

17. Should I check my credit report?

You should monitor your credit report regardless of whether your information has been exposed or you think you may be a victim of identity theft or fraud. Every U.S. consumer over the age of eighteen can receive one free credit report every twelve months by contacting one of the three national credit bureaus or through the Annual Credit Report Service by visiting www.annualcreditreport.com or calling toll-free, 1-877-322-8228.

18. I think I may be a victim of identity theft. What should I do?

In the unlikely event that your information is misused, a CyberScout personal advocate will work with you from the first call you make to report the problem until the crisis is resolved. CyberScout will notify the appropriate agencies, businesses, and institutions, and will make a comprehensive case file.

19. I want to speak with someone at Franklin / I am with law enforcement / I am with the media.

Please contact Transunion at 1-833-367-5713 for assistance or for any additional questions you may have. Should you have additional questions after that, please contact the Franklin IT Department at 414-427-7646.