1. **What happened?**
   On or about October 4, 2023, Richland County detected unauthorized access to our network. Upon learning of this, we promptly took steps to secure our network and safeguard our data, alerted law enforcement and launched a thorough investigation in consultation with external cybersecurity and data privacy experts. After an extensive forensic investigation and manual document review, on August 1, 2024, we discovered that certain files containing personal information may have been accessed and/or acquired by an unauthorized individual between September 28, 2023, and October 26, 2023.

2. **Who is responsible for this?**
   Our thorough investigation determined that an unauthorized individual may have accessed and/or acquired certain files. We do not know the identity of the unauthorized individual, but we have confirmed the security of our network and are confident the incident has been contained and remediated.

3. **Why did it take so long to send notification letters?**
   IBM's Cost of a Data Breach Report 2023, which examined 553 organizations in 16 countries, found that it took an average of 320 days to identify and contain a data security incident and notify affected individuals.

   In our case, as soon as we learned of the incident, we launched an extensive forensic investigation and manual document review. The investigation process took approximately ten months to complete. We take the security of your information very seriously and needed to be sure we were confident in the results of the investigation. Anyone who has experienced a cyber incident knows it is a time-intensive process.

   In accordance with direction from our outside legal counsel and data privacy experts, and Richland County did not notify potentially affected individuals until we determined the names of those involved compromised and what kinds of data may have been accessed and/or acquired. This also aligns with cybersecurity best practices.

4. **Why didn't you tell us as soon as you knew of the cyber incident?**
   When cyber incidents occur, response teams do not have a full understanding of who was affected and what data was involved for the first few days, weeks and even months. Following guidance from our outside legal counsel, we took steps to investigate the incident and provide the most complete and accurate information to potentially affected

individuals as quickly as possible and avoid creating what could have been unnecessary panic. We wanted to have all the information necessary to address individual questions and be able to provide support, like credit monitoring, to those who were affected.

5. **What is Richland County doing to ensure this doesn't happen again?**
   We take the privacy and security of the information entrusted to us very seriously. While we have safeguards in place to protect the data in our care, we are working to review and further enhance these protections. We are taking the necessary steps to best prevent a similar incident from occurring in the future. We also hear and value your feedback as members of our community and are learning from the thoughts and concerns many of you have shared.

6. **How do you know my data hasn't been used for identity theft and/or fraud?**
   At this time, we have no evidence that your information has been used for identity theft or financial fraud as a result of this incident. To date, we have not had any reports of identity theft from members of our community. Out of an abundance of caution, we wanted to make individuals aware of the incident and provide information on steps they can take to safeguard their information.

   Individuals are encouraged to take steps to protect themselves against identity fraud, including placing a fraud alert/security freeze on their credit files, obtaining free credit reports and remaining vigilant in reviewing financial account statements and credit reports for fraudulent or irregular activity on a regular basis.

7. **How will I know if my information was used by someone else?**
   We have no evidence that your information has been or will be used by someone else as a result of this incident. The Federal Trade Commission has published tips for people on protecting their identity. These tips include warning signs of identity theft and can be found on the FTC website at www.ftc.gov/idtheft.

   We also encourage individuals who received notification letters to enroll in the complimentary credit monitoring services offered by Richland County, which help identify and resolve any potential identity theft.

8. **Why did I get a letter with the wrong name/address?**
   We chose to be overly inclusive and over-notify rather than under-notify to ensure we reached every individual who may have been affected. Our notification tracking system is very good, but it is not perfect. As such, we are aware that a few one-off mistakes were made. If you received a letter that you know is inaccurate, please discard it or deliver it to County Administration.

9. **Is it safe to use Richland County's website online services?**
   Yes, it is safe to access and use our online resources. Richland County remains fully functional and operational, and our services were not affected by this incident.

10. **Did you get outside assistance to respond to this incident? Who was involved?**
    Yes. Upon learning of the incident, we promptly engaged outside legal counsel and a leading third-party team of cybersecurity professionals with extensive experience in this area. We also alerted law enforcement.

If you have further questions about this incident, please reach out to Richland County directly at 608-649-3001.