1. **What happened?**
   On the morning of August 4, Advanced's IT teams identified disruptions to our Health and Care environments. These disruptions have since been determined to be the result of a cybersecurity incident caused by ransomware.

   Upon discovering the incident, Advanced immediately took action to mitigate any further risk by isolating our Health and Care environments, where the incident was detected. As a result, certain infrastructure was taken offline.

   The customer groups impacted either directly or indirectly are Adastra, Caresys, Odyssey, Carenotes, Crosscare, Staffplan and eFinancials. All other products are unaffected.

2. **How far away are we from normal service being resumed?**
   In the time since the attack, we have progressed our recovery and restoration efforts with respect to affected systems.

   We have been working with the NHS and the NCSC to validate the additional security measures we have put in place.

   a. For **hosted Adastra** customers:
      - For updates on Adastra, please visit https://www.oneadvanced.com/cyber-incident/adastra/

   b. For **hosted eFinancials** customers:
      - For updates on eFinancials, please visit https://www.oneadvanced.com/cyber-incident/efinancials/

   c. For **hosted Carenotes** customers:
      - For updates on Carenotes, please visit https://www.oneadvanced.com/cyber-incident/carenotes/

   d. For **hosted Staffplan** customers:
      - For updates on Staffplan, please visit https://www.oneadvanced.com/cyber-incident/staffplan/

   e. For **hosted Caresys** customers:
      - For updates on Caresys, please visit https://www.oneadvanced.com/cyber-incident/caresys/

   f. For **hosted Crosscare** customers:
      - For updates on Crosscare, please visit https://www.oneadvanced.com/cyber-incident/crosscare/

   We understand that not all of the service restoration timelines are ideal. We take our responsibility to you very seriously, and we regret and empathise with the disruption you have faced.

3. **What's taking so long to resume normal service?**
   For Staffplan, Crosscare and Caresys, a number of factors have meant that restoration has been more complex than we initially anticipated. We understand that this timeline for restoration of your service is not ideal. We take our responsibility to you very seriously, and we regret and empathise with the disruption you have faced.

4. **Have you contacted the ICO?**
   We are collaborating with the ICO on this issue and will continue to brief them as we learn more information.

5. **Was this a ransomware attack?**

Yes, this was a ransomware attack conducted by a threat actor that we believe, based on threat intelligence provided to us from the regulators and our expert advisors to date, is purely financially motivated.

6. **Which external advisers are assisting you in your response?**
   We moved swiftly to engage leading third-party forensic partners, including Mandiant and Microsoft DART, to conduct a thorough investigation into the incident, which continues to be ongoing. We, alongside our third-party experts, have been and continue to be in contact with the NHS, NCSC, the NCA and other governmental entities, validating our response strategy and providing them with regular status updates on the progress we are making.

7. **Is it safe to continue doing business with you?**
   As a result of the mitigation efforts deployed by our Incident Response Team, our third-party advisors have found no evidence to suggest that customers' systems are at risk of malware spread. Since we isolated our Health and Care systems, we can confirm that the incident has been contained, and no further issues have been detected by our active security monitoring tools.

8. **Where should we go if we need more information?**
   Please check our webpage dedicated to this incident for regular status updates: https://www.oneadvanced.com/cyber-incident/. If you have more specific questions, please reach out to your normal Advanced point of contact.

9. **Is sensitive data at risk as a result of the incident?**
   With respect to potentially impacted data, our investigation is underway, and when we have more information about potential data access or exfiltration, we will update customers as appropriate. Additionally, we will comply with applicable notification obligations.

10. **What are you specifically doing to restore service? What is taking so long?**
    After directly impacted systems were taken offline and additional security measures were put in place, we moved swiftly to engage leading third-party forensic partners, including Mandiant and Microsoft DART, to conduct a thorough investigation into the incident, which is ongoing. These efforts, alongside of our third-party experts, have been progressing, although we recognise the frustration this down time has caused for many of our Health and Care customers. Please rest assured that we are continuing to work around the clock to remediate affected systems and, in some cases, have completely rebuilt them in separate and secure environments.

    To further assure customers of the security of our systems and help them feel confident in reconnecting to our products, we have required all impacted environments to be systematically reviewed prior to going online. This defined process includes:

    - Implementing additional blocking rules and further restricting privileged accounts for Advanced staff;
    - Scanning all impacted systems and ensuring they are fully patched;
    - Resetting credentials;
    - Deploying additional endpoint detection and response agents; and
    - Enhancing 24/7 monitoring capabilities.

    Again, we are prioritising safety and security in every decision we make and go about our restoration process with both diligence and rigor.