1. **What happened?**

   Advanced recently experienced a disruption to our systems that we have since determined to be the result of a cybersecurity incident caused by ransomware. On August 4, 2022, at approximately 7 am, our teams identified the cybersecurity incident. In response, we immediately took action to mitigate any further risk to our customers and isolated all of our Health and Care environments, where the incident was detected.

   As a result, there has been a temporary loss in service to infrastructure hosting products used by our Health & Care customers.

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

   Since these systems were isolated, no further issues have been detected and our security monitoring continues to confirm that the incident is contained, allowing our recovery activities to move forward.

2. **How far away are we from normal service being resumed?**

   With respect to the NHS, we are working with them and the NCSC to validate the additional steps we have taken, at which point the NHS will begin to bring its services back online. For NHS 111 and other urgent care customers using Adastra and NHS Trusts using eFinancials, we anticipate this phased process to begin within the next few days. For other NHS customers and Care organisations our current view is that it will be necessary to maintain existing contingency plans for at least three to four more weeks. We are working tirelessly to bring this timeline forward, and while we are hopeful to do so, we want our customers to be prepared. We will continue to provide updates as we make progress.

3. **What's taking so long to resume normal service?**

   We are rebuilding and restoring impacted systems in a separate and secure environment. To help all customers feel confident in reconnecting to our products once service is restored, we have implemented a defined process by which all environments will be systematically checked prior to securely bringing them online. This 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;
   - Conducting 24/7 monitoring.

   Once these measures have been taken, we will bring environments online and assist customers in reconnecting safely and securely as part of a phased return to service.

4. **Have you contacted the ICO?**
   We have been in contact with the ICO and will continue to be responsive to any questions they may have. We also remain in contact with the NHS, NCSC, and other governmental entities and are providing them with regular status updates.

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 authorities and our expert advisors to date, is purely financially motivated.

6. **Was this incident caused by a state-sponsored actor or connected to recent geopolitical events?**
   Based on threat intelligence provided to us from the authorities and our expert advisors to date, we believe this threat actor to be purely financially motivated.

7. **Which external advisers are assisting you in your response?**

   We moved swiftly to engage leading third-party forensic partners including Mandiant and the Microsoft DART teams to conduct an investigation and ensure that our systems are brought back online securely with enhanced protections. Moreover, we remain in contact with the NHS, NCSC, and other governmental entities and are providing them with regular status updates. We have also been in contact with the ICO and will continue to be responsive to any questions they may have.

8. **Is it safe to continue doing business with you?**

   We want to stress that there is nothing to suggest that our customers are at risk of malware spread and believe that early intervention from our Incident Response Team contained this issue to a small number of servers.

9. **Where should we go if we need more information?**
   Please check this webpage for regular status updates. If you have more specific questions, please reach out to your normal Advanced point of contact. For media inquiries, please see contact details below on this webpage.

10. **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.