PENALTY NOTICE

ADVANCED COMPUTER SOFTWARE GROUP LIMITED

ADVANCED HEALTH AND CARE LIMITED

ASTON MIDCO LIMITED

26 MARCH 2025

DATA PROTECTION ACT 2018

ENFORCEMENT POWERS OF THE INFORMATION COMMISSIONER

PENALTY NOTICE

To: Advanced Computer Software Group Limited
Advanced Health and Care Limited

Of: The Mailbox Level 3, 101 Wharfside Street, Birmingham, United Kingdom, B1 1RF

And

To: Aston Midco Limited

Of: 26 New Street, St Helier, Jersey, JE2 3RA

I. INTRODUCTION AND SUMMARY

1. Pursuant to section 155(1) of the Data Protection Act 2018 ("**DPA**"), the Information Commissioner ("**the Commissioner**"), by this written notice ("**Penalty Notice**") requires Advanced Computer Software Group Limited ("**ACSG**"), Advanced Health and Care Limited ("**AHC**") and its parent company, Aston Midco Limited ("**Aston**" – collectively referred to as "**Advanced**") to pay the Commissioner £3,076,320.

2. This Penalty Notice is given in respect of an infringement of the UK General Data Protection Regulation ("**UK GDPR**").[1] This Penalty Notice contains the reasons why the Commissioner has decided to impose a penalty, including the circumstances of the infringement and the nature of the personal data involved.

3. In accordance with paragraph 2 Schedule 16 to the DPA, the Commissioner gave a notice of intent ("**NOI**") to Advanced on 6 August 2024, setting out the reasons why the Commissioner proposed to give Advanced a penalty notice. In that NOI, the Commissioner indicated the amount of the penalty he proposed to impose was £6,090,000.

4. On 23 September 2024, Advanced made written representations about the Commissioner's intention to give a penalty notice. On 25 October 2024, the Commissioner sought clarification on the written representations, which Advanced provided on 22 November 2024.

5. On 14 March 2024, Advanced entered into a settlement agreement with the Commissioner to resolve this investigation. Advanced acknowledged the Commissioner's decision and agreed to pay a penalty of **£3,076,320**. This Penalty Notice takes into account the written representations from Advanced on the NOI and penalty calculation and where appropriate makes specific reference to them. As part of the settlement, Advanced has agreed not to appeal this Penalty Notice.

---

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018. For the period 25 May 2018 to 31 December 2020, references in this Penalty Notice to the UK GDPR should be read as references to the GDPR (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data) as it applied in the UK during that period.

6. The penalty includes a 20% reduction following a voluntary settlement with the Commissioner.

7. The Commissioner finds that between 25 May 2018[2] and 22 August 2022[3] ("**the Relevant Period**") Advanced infringed Article 32(1) UK GDPR for the reasons set out in this Penalty Notice. In summary:

   a. AHC failed to implement appropriate technical and organisational measures in processing personal data, including special category data, on behalf of data controller customer entities, which left the security of this data at risk.

   b. Advanced's technical and organisational measures, particularly with regards to parts of their AHC IT environment, fell short of fundamental cyber security principles, with deficiencies found in respect of vulnerability scanning, patch management and multi-factor authentication ("**MFA**").

   c. As a consequence, personal data, including special category data such as medical and health-related records, relating to 82,946 individuals, (74,584 of which were associated with UK based data controllers) were exfiltrated by an attacker ("**Threat Actor**") who gained unauthorised access to AHC's IT environment via a ransomware attack between 2 to 4 August 2022 ("**the Incident**").

   d. The personal data of 79,404 data subjects was exfiltrated during the Incident. Of those data subjects, 41,196 had special category data exfiltrated (38,208 did not).[4]

[2] The date of commencement of the DPA and application the GDPR.
[3] The date the first data controller customer entity was reconnected to the relevant system.
[4] Advanced NOI Representations dated 23 September 2024.

e. The data exfiltrated by the Threat Actor included details of how to gain entry to the homes of 890 data subjects ("**home access information**").

f. The data exfiltrated was linked to 16 data controller customers. Overall, 658 data controller customers were impacted by the unavailability of products following the containment actions taken by Advanced to limit any further impact.

g. Data controllers, particularly those offering healthcare services which form part of the UK's Critical National Infrastructure, such as NHS 111, suffered disruption, and faced delays in accessing information during the Incident and for some time afterwards.

h. Following the Incident, Advanced proactively took multiple systems offline to re-build them from the ground up and reconnect data controllers one by one. The first data controller was reconnected on 22 August 2022 and the final data controller was reconnected on 23 May 2023.

i. Other systems outside of Advanced's Health and Care environment were also made unavailable due to containment measures implemented by Advanced post the Incident.

8. The Commissioner is satisfied that, on the balance of probabilities, during the Relevant Period, AHC failed to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks of varying likelihood and severity for the rights and freedoms of natural persons in breach of Article 32 UK GDPR.

9. For the reasons set out in this Notice, the Commissioner considers a penalty of **£3,076,320** adequately reflects the seriousness of the infringement and is effective, proportionate and dissuasive. It also takes into account Advanced's agreement to settle.

II. RELEVANT LEGAL FRAMEWORK

10. Section 155 DPA provides that, if the Commissioner is satisfied that a person has failed, or is failing, as described in section 149(2) DPA, the Commissioner may, by written notice, require the person to pay the Commissioner an amount in sterling specified in the notice.

11. The types of failure described in section 149(2) DPA include, at section 149(2)(c) *"where a controller or processor has failed, or is failing, to comply with … a provision of Articles 25 to 39 of the UK GDPR … (obligations of controllers and processors)."*

12. Article 32(1) UK GDPR relates to the security of processing and states:

"1. Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) the pseudonymisation and encryption of personal data;

(b) the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;

(c) the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

13. The legal framework for setting penalties is set out in **Section V: Decision to Impose Penalty** below.

III. BACKGROUND TO THE INFRINGMENET

A. Background regarding Advanced

14. Advanced is a sector-focused SaaS provider, headquartered in Birmingham. On its website, Advanced refers to itself as 'OneAdvanced'.[5] It provides information technology services across a wide range of sectors, such as healthcare, the legal industry and the education sector.

15. All UK based employees of Advanced and its subsidiaries, including employees who process data relevant to AHC, are employed by Advanced Business Software Solutions Limited ("**ABBS**"). Employees are allocated to a division or function within the wider business, such as the Health & Care Division (which operates through AHC) but are paid and contracted through ABSS.[6]

16. AHC offers a number of software products to data controller customers including clinical patient management software, electronic patient record software, clinical decision support software, care planning software and workforce management software.

---

[5] Unrivalled sector-specific business software | OneAdvanced.
[6] Letter from Norton Rose Fulbright to ICO dated 4 February 2023, point 6.

17. In relation to the Incident, AHC was acting as a data processor, as defined by Article 4(8) UK GDPR. The Commissioner has therefore considered Advanced's obligations in the context of its role as a data processor only.

B. Processing of Personal Data and Information Security Governance at Advanced

18. The policies, standards and procedures regarding information security governance and data processing are authored and controlled by ACSG for the entire Advanced Group and implemented by the Advanced subsidiaries.[7] The diagram below[8] sets out the relevant boards at Group level who have influence over and create information security policies, and the relevant individuals within each subdivision of Advanced Group [redacted] who are expected to create procedures to implement the policies for their division:

[redacted]

[7] Letter from Norton Rose Fulbright to ICO dated 4 February 2023, point 21.
[8] Provided as appendix 2.1 to Letter from Norton Rose Fulbright to ICO dated 4 February 2023.

19. At the time of the Incident, Advanced had several functions at Group level relevant to the processing of personal data and information security governance. The relevant decision-making bodies are as follows:[9]

a. [redacted]

b. [redacted]

c. [redacted]

20. The policies created and controlled by Advanced at the time of the Incident were intended to apply across all of the Advanced legal entities and create a set of baseline policies to be applied across the Advanced Group to ensure standardisation.[10]

C. *Relevant Policies, Procedures and Standards Prior to and During the Incident*

21. The key information management policies relevant to the Incident are set out below:

[9] Letter from Norton Rose Fulbright to ICO dated 4 February 2024, point 6.
[10] Letter from Norton Rose Fulbright to ICO dated 4 February 2023, point 6.

a. [redacted]

b. [redacted][11]

c. [redacted]

D. *Relevant Events Prior to the Incident*

22. [redacted].[12]

23. [redacted].[13]

24. One of the vulnerabilities [redacted] was a lack of mature vulnerability management scanning mechanisms, [redacted].[14]

25. [redacted]

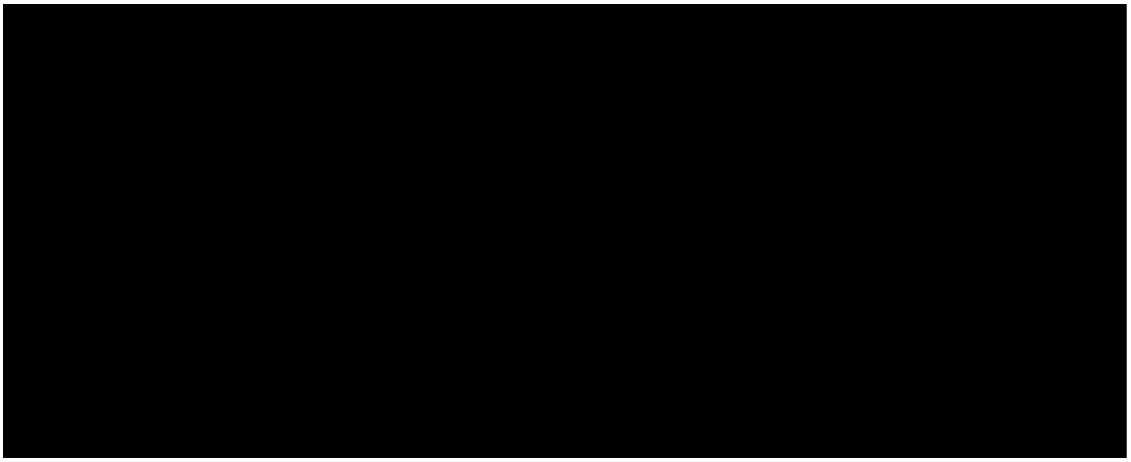
---

[11] [redacted]

[12] [redacted]

[13] Letter from Norton Rose Fulbright to ICO dated 9 October 2022, point 23.

[14] [redacted]



26. [redacted] vulnerability scanning was rated as (jointly) the highest priority security risk to the IT infrastructure.[15]

27. Separately, on 11 August 2020 Microsoft released a security update including a patch for a critical vulnerability in the NETLOGON[16] protocol (known as ZeroLogon CVE-2020-1472).[17] The ZeroLogon vulnerability can allow a cyber threat actor to bypass authentication and gain administrator-level privileges on the domain. Microsoft produced detailed guidance on how to address the vulnerability.[18] Any patch released by Microsoft on 11 August 2020 or later would have addressed this particular vulnerability.

28. The NCSC also published an alert regarding the ZeroLogon vulnerability on 25 September 2020[19] with advice that the vulnerability was being actively exploited and organisations should

---

[15] [redacted]
[16] The NETLOGON is a Local Security Authority service that authenticates users into the domain.
[17] CVE-2020-1472 - Security Update Guide - Microsoft - Netlogon Elevation of Privilege Vulnerability
[18] How to manage the changes in Netlogon secure channel connections associated with CVE-2020-1472 - Microsoft Support
[19] Alert: UK organisations should patch Netlogon... - NCSC.GOV.UK

install necessary updates as soon as possible. A further security update was made available by Microsoft in February 2021.

29. The National Institute of Standards and Technology ("**NIST**") graded the ZeroLogon vulnerability with a CVSS v3 10.0/10.0 which made it one of the most serious, active vulnerabilities in existence.[20]

E. The Incident – 2 to 4 August 2022

30. An [redacted] forensic investigation [redacted][21] ("the **Forensic Investigation**") established the following in relation to the Incident:

a. The earliest evidence of Threat Actor activity occurred on 2 August 2022, at 20:50:48, when the Threat Actor first logged into AHC's Staffplan system [redacted] Citrix.[22] Authentication to the Staffplan environment via Citrix was provided using a username and password; despite extensive enquiries, it is not known how the credentials, [redacted].[23]

b. From this initial foothold, the Threat Actor utilised techniques to pivot further into AHC's IT environment.

c. At 02:21:52 on 3 August 2022, a file was likely executed to exploit ZeroLogon vulnerability. From this point the Threat

[20] NVD - CVE-2020-1472 (nist.gov).
[21] [redacted]
[22] Citrix is a software that allows remote access to servers.
[23] Letter Norton Rose Fulbright to ICO 9 October 2022, point 12.

Actor was able to escalate their privileges to a domain administrator account.

d. Between 02:24:33 on 3 August 2022 and the early hours of 4 August 2022, the Threat Actor leveraged the domain administrator account to traverse through numerous Advanced domains, disabled antivirus software and performed additional reconnaissance and exploration of resources. During this period, the Threat Actor also navigated to cloud storage and file hosting services and downloaded infrastructure management utilities that enabled them to exfiltrate data.

e. The Threat Actor also deployed ransomware, with the earliest evidence of execution taking place on 4 August 2022 at 02:05:10.

f. The last evidence of Threat Actor activity was seen at 08:13:36 on 4 August 2022.

g. Approximately 395 endpoints were infected by the Threat Actor during the intrusion.

h. Approximately 19GB of data had been exfiltrated.

31. Advanced identified evidence of compromise in the early hours of 4 August 2022.

F. How the Incident Came to the Commissioner's attention

32. The UK GDPR does not impose any obligations on data processors to notify the Commissioner of a personal data breach.

33. The ICO contacted Advanced on 5 August 2022 following widespread media reports of disruption to NHS services. Advanced responded to the ICO on the same day and has continued to cooperate with the ICO's investigation.

G. Post-Incident Response

34. On the day the Incident was discovered, Advanced promptly instructed [redacted] investigators to determine the extent of compromise in the Health & Care Division environment and to provide assurance that other Advanced environments were not compromised. Advanced also engaged [redacted] to support the initial rebuild and investigation activities of the impacted domains. [24]

35. The Incident affected the availability of 9 AHC customer products[25] for approximately 658 data controller customers.[26] Out of the 9 products, 3 were taken offline as a precautionary measure but were not directly impacted by the ransomware [redacted]. Details of the remaining 6 products directly impacted by the Incident are set out below:[27]

[redacted]

[24] [redacted]

[25] [redacted].

[26] Letter from Norton Rose Fullbright to ICO dated 2 February 2024, point 4.

[27] Letter from Norton Rose Fullbright to ICO dated 2 February 2024, response to Q4.

36. Other systems outside of the Health & Care Division environment (still controlled and operated by Advanced) were also made unavailable due to the containment measures implemented by Advanced in response to the Incident. However, there is no evidence that these were infected with ransomware or accessed by the Threat Actor.

37. Advanced notified all potentially impacted data controller customer entities on 5 August 2022.

38. Following discovery of the Incident, Advanced worked with the relevant stakeholders to plan restoration of the impacted products. The planning and implementation of the rebuilding program began on 4 August 2022 (with Adastra), and involved consultation with NHS Digital, NHS Nations and the NCSC.[28] The period of controller customer unavailability ranged from 18 days to 284 days, depending

[28] Letter from Norton Rose Fulbright to ICO dated 9 October 2022, point 14.

on the product. By 15 May 2023, all of Advanced's controller customers were able to access the relevant products.

39. Advanced has provided the Commissioner with details of the considerable improvements it has made to its systems following the Incident.[29] Advanced also employed a new Chief Information Security Officer and Chief Technical Officer to oversee security.[30]

H. Exfiltration of Personal Data

40. It is understood that personal data was exfiltrated from Staffplan and Caresys only with 16 data controllers impacted.[31]

I. Reported Impact on Data Controllers and Data Subjects and Disruption to Services

41. At the time of the Incident, and for some months after, there were media reports of disruption to NHS and other healthcare services. [32]

42. In a report dated 28 September 2022,[33] the Chief Executive of the Oxford Health NHS Foundation Trust reported on the Incident to the Board Directors stating:

---

[29] Letter from Norton Rose Fulbright to ICO dated 2 February 2024, point 7.
[30] Letter from Norton Rose Fulbright to ICO dated 2 February 2024, point 16.
[31] Letter from Norton Rose Fulbright to ICO dated 9 October 2022, point 1.
[32] GPs told to expect influx of calls from patients redirected due to 111 outage - Pulse Today; NHS 111 expects delays after cyber-attack causes system outage | NHS | The Guardian., NHS IT supplier held to ransom by hackers - BBC News; Fears for patient data after ransomware attack on NHS software supplier | NHS | The Guardian; Advanced cyber-attack: NHS doctors' paperwork piles up - BBC News; Oxford Health: Cyber attack continues to hit NHS trust's services - BBC News; Mental health trusts still unable to access records months after attack (digitalhealth.net); NHS cyber attack hits patient care with records left in 'chaos' three months on (inews.co.uk).
[33] 59_BOD_CEO-BoD-report-SEPT2022-Final-v.4.docx (live.com).

"On the 4th of August, a cyber attack on Advanced Systems Ltd resulted in the loss of access to a number of our key electronic records systems, including Adastra and Carenotes. The incident was originally managed as an IM&T Serious Incident but was upgraded to a Trust wide Critical Incident on the 9th of August. This was a national incident affecting a number of other NHS organisations. The vast majority of the Trust's clinical services along with a number of financial services were impacted and as a result a variety of business continuity measures were put in place in keeping with our emergency response protocols. The outage extended to both mental health and physical health services.

As a consequence of a huge amount of effort from colleagues across Oxford Health we were able to maintain services although in a sub-optimal manner. At the time of writing, Carenotes, our most significant electronic patient record system, remains out of action. We continue therefore continue[sic] *to work closely with NHS England and other affected trusts in order to develop and maintain suitable contingency arrangements.*

This ongoing cyber incident has placed a huge burden on colleagues across Oxford Health, many of whom have worked considerably in excess of their contracted hours in order to deliver services."

43. Although the level of any actual harm to data subjects is difficult to quantify, given the integral nature of electronic records to patient care, the Incident 'reportedly' had a significant impact on patient care and according to the Oxford Health Report quoted above placed a "*huge burden*" on that health provider.

IV. THE COMMISSIONER'S FINDINGS OF INFRINGEMENT

A. Advanced's role as a data processor and Jurisdiction

44. AHC was acting as a processor of the relevant personal data on behalf of data controllers within the meaning of Article 4(8) UK GDPR.[34]

45. Advanced is established in the UK and the relevant processing of personal data took place in the UK and therefore the UK GDPR applies to this processing pursuant to Article 3(1) UK GDPR.[35]

B. Personal Data affected by the Incident

46. 16 UK based data controllers had data exfiltrated as part of the Incident, with a further three data controllers based in Ireland.

47. Personal data of 82,946 individuals were exfiltrated, of which 74,584 were associated with UK-based data controllers. Some of those individuals were deceased, which reduces the number of data subjects whose data was exfiltrated to 79,404. These data subjects are customers, patients or other relevant data subjects for the impacted data controllers. Advanced states that there were likely further duplicates within this figure, however it could not deduplicate further with real accuracy. Of those data subjects, 41,196 had special category data exfiltrated (38,208 did not).

[34] Letter from Norton Rose Fulbright to the ICO dated 4 February 2023, point 25 refers to a Master Agreement (Appendix 7.1) which is used as standard in contracts entered into between the Advanced Group and customers. The Commissioner notes that the Master Agreement refers to Advanced (or the entity from the Advanced Group as referred to in the Order Form) as the processor.

48. Advanced has confirmed that the following categories of data were exfiltrated as part of the Incident: [36]

    a. **Demographic and contact information**, including: name, date of birth, postal address, personal telephone number, and personal email addresses.
    b. **Employment-related information**, including: employer name, job title, employee ID, salary details, business email address, business telephone number.
    c. **Medical or health-related information**, including: medical records, medical history, medical record number, treatment, diagnosis, prescription information, NHS number and date of treatment/date of service.
    d. **Other information (including special category data)**, including: UK National Insurance number, home access information, racial or ethnic origin, religion or philosophical beliefs, and nationality.

49. The data exfiltrated as part of the data breach is personal data within the meaning of Article 4(1) UK GDPR and section 3(2) DPA. Furthermore, some of the data exfiltrated would also be considered special category data within the meaning of Article 9(1) UK GDPR. Of note, the home access information of 890 data subjects was exfiltrated.

C. The Infringement

50. The Commissioner has considered whether the facts set out at paragraphs 14 – 43 above constitute an infringement of the UK GDPR.

---

[36] Letter Norton Rose Fulbright to ICO dated 9 October 2022, point 1

51. For the reasons set out below, the Commissioner's view is that AHC has infringed Article 32(1) UK GDPR. The infringement involved failures by Advanced to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk posed by processing in the following areas:

    a. Vulnerability management, encompassing:
        i. Vulnerability Scanning
        ii. Patch Management; and
    b. Risk Management (relating to MFA)

52. The Commissioner finds that these failures significantly contributed to a Threat Actor gaining unauthorised access to AHC systems and exfiltrating personal data, including special category data.

(a)(i) Vulnerability Management – Vulnerability Scanning

53. According to the NCSC, vulnerability scanning is a broad term, used to describe the automated process of detecting defects in an organisation's security program. Vulnerability scanning solutions can be an affordable way to automatically detect security issues within an organisation's network as part of an effective vulnerability management programme.

54. There were numerous Advanced products and systems processing significant volumes of personal data and special category data within the AHC environment including [redacted]. Advanced has not provided any evidence to demonstrate that regular vulnerability scanning was taking place in relation to these products and across the AHC environment.

55. Advanced was aware of the need to undertake vulnerability scanning as it was an area of significant risk [redacted].

56. [redacted] rated vulnerability scanning as the highest priority security risk to the IT infrastructure.[37] [redacted][38] The Commissioner therefore considers that Advanced was aware of the risks posed by the lack of vulnerability scanning.

57. Advanced previously recognised the need for further in-house penetration testing and vulnerability scanning to be deployed across its entire IT infrastructure and such tools were deployed in the corporate environment.[39]

58. Advanced had procured a vulnerability scanning application in [redacted], a web application scanning in [redacted] and a policy compliance application in [redacted] prior to the Incident. However, no vulnerability scans or policy compliance scans were conducted using these applications in the AHC environment prior to the Incident. Only two web application scans were conducted in the AHC environment.[40] There was therefore limited visibility of vulnerabilities that existed in the AHC environment prior to the Incident.

59. The failure to undertake adequate vulnerability scanning within the AHC environment was contrary to [redacted]

---

[37] [redacted]

[38] Letter from Norton Rose Fulbright to ICO dated 2 February 2024, point 15a

[39] Letter from Norton Rose Fullbright to ICO dated 9 October 2022, point 23.6.

[40] Advanced stated that the Qualys Web Application scans were conducted 'across limited parts of the internet-facing AHC IT estate' namely in Odyssey on 19 May 2022 and CareCloud on 25 April 2022 - Letter from Norton Rose Fulbright to ICO dated 4 February 2023, point 10.

[redacted] dated 25 June 2020 [redacted]

[redacted]."[41]

60. [redacted] applied to the entire IT infrastructure of Advanced,[42] and therefore applied to AHC. The evidence before the Commissioner is that this policy was not being implemented in the AHC environment.[43]

61. The NCSC state that organisations should aim to perform vulnerability scans of infrastructure on a regular basis (at least once every month), or immediately after applying changes to remediate a critical issue.[44] The evidence shows that scans were not taking place in the AHC environment on a regular basis, and certainly not once a month as advised by the NCSC.[45] The Commissioner notes vulnerability scans were conducted on a regular basis in Advanced's corporate environment.[46]

62. Advanced provided the Commissioner with copies of penetration test reports that included vulnerability scanning as part of the engagement scope, however conducting scans as part of penetration test does not exclude the requirement for ongoing, regular scanning mechanisms.

---

[41] [redacted]

[42] [redacted]

[43] Response to IN dated 4 February 2023, point 10.

[44] Vulnerability scanning tools and services - NCSC.GOV.UK.

[45] Letter from Norton Rose Fulbright to ICO dated 9 October 2022, point 3, Appendix 1.1.

[46] Letter from Norton Rose Fulbright to ICO dated 2 February 2024, point 14b.

63. Furthermore, the evidence provided by Advanced in relation to penetration tests in the AHC environment shows that these were infrequent for each product and could not be relied upon to serve the same purpose as a regular ongoing vulnerability scanning programme. Where penetration tests were conducted, some of these revealed vulnerabilities which were later exploited in the Incident.

64. The forensic investigation determined that privilege escalation to Domain Administrator was likely achieved through exploitation of the ZeroLogon vulnerability.

65. The ZeroLogon vulnerability had been discovered and widely publicised two years prior to the Incident. In an article written by Qualys in September 2020, steps were published on how to remediate the ZeroLogon vulnerability (CVE-2020-1472).[47] Qualys is the same vulnerability management tool deployed by Advanced within the corporate network. Advanced would therefore have had ample opportunity to identify and remediate the high risk ZeroLogon vulnerability had it implemented such scanning in the AHC environment.

66. In light of the above, the Commissioner finds that the failure to implement comprehensive vulnerability scanning in the AHC environment amounted to a failure to implement appropriate technical and organisational measures to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services (Article 32(1)(b) UK GDPR), and to ensure a process for regularly testing, assessing and evaluating the

[47] Microsoft Netlogon Vulnerability (CVE-2020-1472 - Zerologon) – Automatically Discover, Prioritize and Remediate Using Qualys VMDR® | Qualys Security Blog.

effectiveness of technical and organisational measures for ensuring the security of the processing (Article 32(1)(d) UK GDPR).

(a)(ii) Patch Management

67. Patch management is essential to ensure that systems have the latest security updates which will often include fixes for various vulnerabilities. Insufficient patch management increases the risk that if such security issues are left unaddressed, the system is more open to exploitation. Effective patch management is essential to ensure these issues are resolved so they cannot be exploited by a threat actor.[48]

68. As referred to at paragraphs 27 - 29 above, the ZeroLogon vulnerability was widely publicised, with repeated messages about ensuring patching as soon as possible. A patch update was made available by Microsoft in August 2020 with a further security update made available in February 2021.

69. [redacted].[49]

70. Advanced undertook some patching activities in response to the ZeroLogon vulnerability (CXVE-2020-1472) but its approach to patching in the AHC environment was ad hoc, as it did not have a mature patch validation process in place.[50]

[48] What Is Patch Management? | IBM.
[49] [redacted]
[50] Letter to Norton Rose Fullbright to ICO dated 9 October 2022, point 4

71. Advanced has been unable to confirm whether the ZeroLogon vulnerability had been patched in the impacted server in the AHC environment prior to the Incident as there was not an accurate record of patching at the time of the Incident. Activities undertaken to restore the servers post incident involved patching the ZeroLogon vulnerability out of the systems, which meant this aspect of the forensic history had been overwritten.

72. Given the findings of the forensic investigation regarding the likely exploitation of ZeroLogon vulnerability, the evidence that Advanced was aware of the vulnerability, the evidence regarding Advanced's "*ad-hoc*" patch management, and the absence of evidence to demonstrate that the ZeroLogon vulnerability had been patched by Advanced before the Incident, the Commissioner finds that Advanced has infringed Article 32(1) UK GDPR. The Commissioner finds that Advanced did not implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk presented by the processing.

73. The Commissioner finds this failure led to an infringement of Article 32(1)(b) UK GDPR, as the failure to have adequate patch management in place led to an inability to ensure ongoing confidentiality, integrity, availability of processing systems and services as demonstrated by the Incident and subsequent exfiltration of personal and special category data.

Vulnerability Management – State of the Art

74. Vulnerability management controls are widely regarded as a foundational element of an effective Information Security Management System (ISMS).

75. ISO27002:2017 section 12.6.1[51] states *"Information about technical vulnerabilities of information systems being used should be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk."*

76. The standard goes on further to state in section 18.2.3 that penetration testing and vulnerability assessments *"can be useful in detecting vulnerabilities in the system and for inspecting how effective the controls are in preventing unauthorized access due to these vulnerabilities".*

77. The NCSC's Cyber Essentials v3.0[52] (the version of Cyber Essentials that was in effect at the time this Incident occurred) states:

"The Applicant must ensure all in scope software is kept up to date. All software on in scope devices must be:

...

updated, including applying any manual configuration changes required to make the update effective, within 14 days of an update being released, where:*

- *The update fixes vulnerabilities described by the vendor as 'critical' or 'high risk'*

[51] ISO/IEC 27002:2022(en), Information security, cybersecurity and privacy protection — Information security controls

[52] Cyber-Essentials-Requirements-for-Infrastructure-v3-0-January-2022.pdf (ncsc.gov.uk)

- *The update addresses vulnerabilities with a CVSS v3 score of 7 or above*
- *There are no details of the level of vulnerabilities the update fixes provided by the vendor"*

78. The Commissioner finds that Advanced's approach to vulnerability management within the AHC environment did not meet these industry wide standards. Advanced has stated that its corporate IT infrastructure was already accredited for Cyber Essentials Plus pre-incident. However, its Advanced Health & Care environment was not.

Vulnerability Management – Costs of Implementation

79. Appropriate vulnerability management controls are standard components of an ISMS that should be accounted for and tailored to organisations of all sizes. The costs of implementation could therefore vary and would not be a factor that would prevent the use of these controls.

80. Advanced is a large organisation with a significant turnover. Advanced was already using Qualys vulnerability management products in the business. Advanced engaged and implemented such controls in the AHC environment post-Incident.[53]

81. The Commissioner therefore considers that the cost of implementation ought not to have been a prohibitive factor in implementing appropriate technical and organisational measures to ensure security of processing of personal data.

[53] Letter from Norton Rose Fulbright to ICO dated 9 October 2022, point 22.

Vulnerability management – nature, scope and purpose of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons

82. AHC was processing significant volumes of personal data, including special category data, on behalf of health and social care data controllers. This data included medical records of vulnerable individuals. This should be considered high-risk processing. The loss of confidentiality, integrity, availability and resilience of this data could, and did, lead to delays in treatment and ultimate risks to the health, safety and wellbeing of data subjects. The Commissioner would therefore expect Advanced to implement appropriate technical and organisational measures to ensure a level of security appropriate to this risk.

83. "Health" has been listed by the Cabinet Office as one of the 13 Critical National Infrastructure sectors. The Commissioner would expect Advanced to be aware of the health sector's status as Critical National Infrastructure and therefore the severity of the risks to the rights and freedoms of natural persons is of the highest level.

84. In summary, the Commissioner finds that the lack of appropriate vulnerability scanning and patch management during the relevant period constitutes an infringement of Article 32(1) UK GDPR. The Commissioner finds that AHC did not implement appropriate technical and organisational measures to protect the personal data, including special category data, being processed.

*b. Risk Management (**MFA**)*

85. AHC did not have MFA in place on their public facing Staffplan Citrix environment at the time of the Incident.[54] The Commissioner note that two applications within the AHC environment (Adastra and Carenotes) had MFA. Advanced estimates that in 2022 it processed the personal data of approximately 25–30 million data subjects in the AHC environment. Adastra and Carenotes, which had MFA, processed approximately 95% of the personal data within the AHC environment. The remaining 5% of personal data processed in the AHC environment did not have MFA.[55] Despite MFA being in place for Adastra and Carenotes, the Threat Actor was able to gain access to the entire AHC environment [redacted].

86. Advanced had already developed an MFA solution (SecurEnvoy) in April/May 2021 which was tested and confirmed to be working. It also had other forms of MFA applied to Carenotes and Adastra. However, MFA was not rolled out to all customers prior to the Incident as Advanced intended to replace the legacy products to which access was being provided via Citrix. Advanced states that previous interactions with customers created the perception that there was an unwillingness to implement MFA due to the operational challenges this would present to the end user, which is further considered at paragraph 122(f).

87. The Commissioner considers that the deployment of MFA would likely have impeded the Threat Actor's ability to access Citrix in the first instance and therefore would have likely prevented the subsequent breaking out of Citrix, as well as the ultimate exfiltration and encryption of personal and special category data.

---

[54] Letter from Norton Rose Fullbright to ICO dated 09 October 2022, point 10.
[55] Letter from Norton Rose Fullbright to ICO dated 22 November 2024.

88. The Commissioner finds the failure to fully implement MFA in the AHC environment constituted a breach of Article 32(1)(b) UK GDPR.

MFA - State of the Art

89. Citrix published guidance in 2016 which states that:

"When considering identity and authentication in a secure environment, multi-factor authentication is recommended. For example, a combination of user name, password, plus additional methods such as hardware or software-based token access. Multi-factor authentication is likely to be mandatory for remote access."

90. The NCSC recommends MFA be used for services such as remote access. Guidance published by the NCSC in 2018 states:

"As long as passwords are used for authentication, there will always be a chance that users and administrators will choose machine-guessable passwords and be susceptible to social engineering. Therefore:

Organisations should choose Cloud and Internet-connected services that offer a form of multi-factor authentication.

All users, including administrators, should use multi-factor authentication when using Cloud and Internet-connected services. This is particularly important when authenticating to services that hold sensitive or private data."

91. The NCSC Cyber Essentials accreditation requires MFA where it is available.[56]

[56] Cyber-Essentials-Requirements-for-Infrastructure-v3-0-January-2022.pdf (ncsc.gov.uk)

92. ICO guidance specifically relating to passwords in online services states *"you should implement two-factor or multifactor authentication wherever it is possible to do so. This will be more important where the personal data that can be accessed is of a sensitive nature, or could cause significant harm if it were compromised."*

93. MFA was a widely utilised industry standard security solution for years prior to the Incident and is considered best practice.

94. The Commissioner finds that AHC failed to meet accepted industry standards with regards to MFA in certain parts of the AHC environment.

MFA - Cost of Implementation

95. For the products not protected by MFA, Advanced has stated that it had a fully tested and working solution for MFA which had been developed prior to the Incident. However Advanced states that this had not been rolled out due to a perception that customers would not be willing to implement MFA because of operational and technical challenges, and due to the inability to unilaterally enforce MFA without customer approvals and consideration of their capabilities and requirements. It is therefore unlikely that the cost of implementation was a prohibiting factor.

MFA - Nature, Scope, Context and Purpose of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons

96. The nature, scope, context and purpose of processing are the same as set out in paragraphs 82 - 83 above. The Commissioner has

received Representations regarding the context in which Advanced's health and care customers operated, and the fact that MFA was not always considered a viable solution (e.g. part- time cleaners, mental health professionals, contract employees without corporate MFA devices).

97. In conclusion, the Commissioner finds that the lack of MFA constitutes an infringement of Article 32(1) UK GDPR. The Commissioner finds that AHC did not implement appropriate technical and organisational measures to protect the personal and special category data being processed.

V. DECISION TO IMPOSE A PENALTY

98. For the reasons set out below, the Commissioner has decided to impose a penalty on Advanced and Aston in respect of the infringement of Article 32(1) UK GDPR.

A. Legal Framework – Penalties

99. When deciding whether to issue a penalty notice to a person and determining the appropriate amount of that penalty, section 155(2)(a) DPA requires the Commissioner to have regard to the matters listed in Article 83(1) and (2) UK GDPR, so far as they are relevant in the circumstances of the case.

100. Article 83(1) UK GDPR requires any penalty imposed by the Commissioner to be effective, proportionate, and dissuasive in each individual case.

101. Article 83(2) UK GDPR requires the Commissioner to have due regard to the following factors when determining whether to issue a penalty

notice and the appropriate amount of any such penalty in each individual case:

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
(b) the intentional or negligent character of the infringement;
(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
(e) any relevant previous infringements by the controller or processor;
(f) the degree of cooperation with the Commissioner, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
(g) the categories of personal data affected by the infringement;
(h) the manner in which the infringement became known to the Commissioner, in particular whether, and if so to what extent, the controller or processor notified the infringement;
(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained,

or losses avoided, directly or indirectly, from the infringement.

B. The Commissioner's decision to impose a penalty

102. Paragraphs 103 - 153 below set out the Commissioner's assessment of whether it is appropriate to issue a penalty in relation to the infringement set out above. This assessment involves consideration of the factors in Articles 83(1) and 83(2) UK GDPR. The order in which these considerations are set out below follows the Commissioner's Data Protection Fining Guidance, dated March 2024 ("**the Fining Guidance**"):[57]
    a. Seriousness of the infringement (Article 83(2)(a), (b) and (g) UK GDPR
    b. Relevant aggravating or mitigating factors (Article 83(2)(c)-(f), (h)-k) UK GDPR)
    c. Effectiveness, proportionality and dissuasiveness (Article 83(1) UK GDPR).

Seriousness of the infringement: Article 83(2)(a) the nature, gravity and duration of the infringement

103. In assessing the seriousness of the infringement, the Commissioner has given due regard to the nature, gravity and duration.

Nature of the infringement

[57] https://ico.org.uk/about-the-ico/our-information/policies-and-procedures/data-protection-fining-guidance/.

104. Article 32 UK GDPR is an important element of the data protection framework established under the UK GDPR. An infringement of this provision is subject to the standard maximum amount.[58]

105. The infringement consisted of a failure to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk taking into account the state of the art, costs of implementation and the nature, scope, context and purpose of its processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons.

106. The Commissioner's view is that the Incident uncovered serious failings in AHC's application of fundamental cyber security principles, and compliance with its own security standards. Had the relevant processing complied with Article 32(1) UK GDPR, the likelihood that personal data, including special category data, would have been compromised during an attack such as this Incident could have been significantly reduced. The failure to implement appropriate measures exposed the significant amount of personal data being processed by AHC to serious risks.

Gravity of the infringement

107. In assessing the gravity of the infringement, the Commissioner has considered the nature, scope and purpose of the relevant processing as well as the data subjects affected by the relevant processing.

108. AHC processes data on behalf of data controller customer entities which includes the personal data of the patients and employees of healthcare organisations. AHC processes some special category data,

[58] Article 83(4)(a) UK GDPR.

including in relation to vulnerable data subjects. AHC also process children's personal data.[59] The data processing which AHC undertakes is the hosting of personal data inputted by data controller customers into AHC products. Hosting, or storage, of personal data is data processing. The processing activities provided by AHC support the delivery of frontline healthcare services which are considered to be Critical National Infrastructure.

109. In the absence of appropriate security measures, the nature of the relevant processing is likely to result in high risk to data subjects.

110. As regards to the scope of processing, AHC was processing significant volumes of personal data (including special category data) in the AHC environment for health and social care data controller customer entities based in the United Kingdom.

111. The purpose of the processing was to host personal data as an aspect of providing clinical management software services to support the provision of health and social care services.[60] AHC's services enable its data controller client entities to process patient medical records and conduct financial management, spend management, governance and risk management and staff HR management. The Commissioner considers this to be a core activity of Advanced, as Advanced's business model relies on providing software services to its data controller customer entities who will require the data to be processed in accordance with Article 32 UK GDPR.

112. The processing, and therefore the infringement, affected Advanced's AHC data controller customer entities, and the individuals who use

[59] Advanced's healthcare data controller customer entities, for example NHS 111 service would process the special category data of children. [redacted]

[60] Healthcare Software | OneAdvanced.

those services. The Incident resulted in the unauthorised exfiltration of personal data of 79,404 data subjects. In addition, there was also reported disruption to healthcare services in the UK, including reported delays to NHS 111. There were reports of healthcare services being unable to access electronic records and having to rely on paper records which could have led to patient harm.[61] There were also reports of continued disruption to healthcare services up until November 2022.[62]

113. The Commissioner is of the view that, on the balance of probabilities, the Incident occurred as a result of the infringement set out in this Notice. In relation to the level of damage suffered by affected data subjects, the Fining Guidance makes clear that the Commissioner will have regard to both potential and actual damage.

114. In assessing the level of damage suffered as a result of the infringement, the Commissioner has had regard to the reported impact of the data breach as well as the potential for damage.

115. The Commissioner acknowledges that he has not received any complaints from data subjects as a result of this incident. Advanced has also confirmed that it has not received complaints from data subjects, nor is it aware of any such complaints from data subjects to data controllers. Advanced has stated that it has dealt with queries and 'complaints' from data controllers amicably and timeously.[63] Advanced also states that it has not received evidence, nor does it hold evidence of harm or damage to individual data subjects arising from the incident. The Commissioner therefore acknowledges that there is no evidence of actual harm to data subjects.

---

[61] Paragraphs 41-43.
[62] Paragraph 41.
[63] Advanced representations dated 22 November 2024

116. However, the Commissioner is also entitled to consider the potential for damage, which includes physical or bodily harm, psychological harm, and loss of human dignity. Data subjects who were subsequently notified of the unauthorised disclosure of their personal data, including their special category data, may additionally have suffered distress and anxiety over the loss of control over such sensitive personal data.

117. The Fining Guidance recognises that some harms are less tangible (for example, distress and anxiety or loss of control over personal data). Furthermore, where an infringement affects a large number of data subjects, it may result in a high degree of damage in aggregate and give rise to wider harm to society. This incident led to the exfiltration of personal data, including special category data and home access information, but also led to reported disruption of healthcare services which form part of the UK's National Critical Infrastructure.

Duration of the infringement

118. The duration of the infringement was from 25 May 2018 (the date of the commencement of the DPA and application of the UK GDPR) until 22 August 2022 when the first data controller was reconnected.

119. The risk of damage (i.e. potential damage) to data subjects existed from at least as early as 25 May 2018 and could have materialised at any point during this lengthy period. The risk materialised on 2 August 2022. The length of the infringement increases the seriousness.

Conclusion on the nature, gravity and duration of the infringement

120. The nature, gravity and duration of the infringement all demonstrate the seriousness of the infringement.

Seriousness of the infringement: Article 83(2)(b) the intentional or negligent character of the infringement

121. There is no evidence to show that AHC acted intentionally in committing the infringement. The Commissioner does, however, find that AHC was negligent (within the meaning of Article 83(2)(b) UK GDPR) in failing to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk that arose from its processing activities in the health and care division.

122. The Commissioner finds that AHC was negligent for the reasons set out below:

a) AHC failed to abide by [redacted];

b) AHC was aware of the need to undertake regular vulnerability scanning [redacted][64] [redacted]

c) Advanced failed to deploy vulnerability scanning in the AHC environment, despite deploying this in the corporate environment;

64 [redacted]

d) AHC was aware of the ZeroLogon vulnerability from August/September 2020, almost two years before the Incident took place. The ZeroLogon vulnerability was widely publicised in the cybersecurity industry and the relevant patches were made available by Microsoft in 2020 and 2021. AHC was aware of the need to patch the vulnerability however it appears no checks were undertaken to confirm the patch had been applied in the AHC environment, or if it had been applied, that the patch was working by the time of the Incident;

e) AHC ought to have been aware of the Microsoft, NCSC and NIST alerts referred to in paragraphs 28 - 29 above, and therefore ought to have been aware of the severity of the risk posed by the ZeroLogon vulnerability and the need to implement the relevant patches as soon as practicable;

f) Advanced had the capabilities to implement MFA across all products in the AHC environment but state that they did not do so due to a perceived reluctance on the part of their data controller customer entities. While Advanced was unable to evidence this reluctance on the part of their customers prior to the incident, in any case, the Commissioner's view is that this is not an acceptable reason not to implement, nor to advise data controller customers to implement,[65] such a fundamental security measure, particularly when considering the sensitive nature of the data Advanced was processing.

---

[65] Pursuant to Article 28(3)(f) UK GDPR *assist the controller in ensuring compliance with the obligations pursuant to Articles 32 to 26 taking into account the nature of processing and the information available to the processor.*

123. The Commissioner received representations from Advanced regarding the practical feasibility of deploying MFA and vulnerability scanning across the AHC environment. The Commissioner recognises that there may have been some complexity in implementing these measures, given the nature of AHC's technical environment. However, the Commissioner remains of the view that this was achievable and ought to have been implemented, given the nature of the processing and the risks to data subject as already outlined.

124. The Commissioner considers AHC was negligent, which increases the seriousness of the infringement.

Seriousness of the infringement: Article 83(2)(g) categories of personal data affected

125. The categories of personal data affected by the infringement are also relevant to the assessment of seriousness. As identified in paragraph 48, AHC was processing special category data within the AHC environment. The data exfiltrated by the Threat Actor also included special category data.

126. The Commissioner considers infringements involving the processing of special category data particularly serious.[66]

Conclusions on seriousness of infringement

127. Having considered the nature, gravity and duration of the infringement, and the categories of personal data affected, the

[66] Fining Guidance, paragraph 71.

Commissioner categorises the infringement as having a high degree of seriousness.

128. In the absence of any mitigating factors, the infringement would warrant a monetary penalty. The Commissioner's consideration of any aggravating or mitigating factors follows below.

Relevant aggravating or mitigating factors: Article 83(2)(c) any action taken by the controller or processor to mitigate the damage suffered by the data subjects

129. Advanced undertook the following steps to mitigate the damage suffered by data subjects:

- Immediate incident response by isolating the AHC environment to limit the scope of potential damage;
- Notifying all customers of the incident within 24 hours of discovery irrespective of whether they were affected;
- Working with the National Cyber Security Centre ("**NCSC**") and NHS Digital as part of its remediation and recovery plan;
- Dedicating a team of 18 people to infrastructure restoration and engaging third party experts as part of the Forensic Investigation and analysis of the data impacted;
- Dedicating resources to implement mechanisms whereby records of data were made available to affected controllers during the outage, including one-to-one contact with customers where needed;
- Working with the affected data controllers to implement a mechanism whereby records that were generated during the outage could be imported into the systems once they had been brought back online, to mitigate the risk of personal data being lost as organisations migrated back to using AHC services;

- Undertaking a comprehensive review of potentially impacted data, and notification to impacted controllers; and
- Providing impacted data controllers with data subject notification templates including remedial advice data subjects could take to protect themselves. These notifications were prioritised based on the sensitivity of the data sets.

130. Advanced submits that overall incident remediation and response costs were in excess of £21 million. Overall, the Commissioner considers the incident response and remediation action undertaken by Advanced to be a mitigating factor.

Relevant aggravating or mitigating factors: Article 83(2)(d) the degree of responsibility of the controller or processor

131. The Commissioner considers that it would have been proportionate for AHC as the data processor to have fully implemented fundamental cyber security measures across its entire AHC environment to protect the personal data it processed on behalf of its data controller customer entities. The Commissioner also takes into account Advanced's size, the number of data controller customer entities it processed data on behalf of and the volume and nature of personal data it processed.

132. Article 32 UK GDPR requires organisations to implement appropriate technical and organisational measures to ensure a level of security appropriate to the risks presented by their processing; to include the potential impacts these risks may have on the rights and freedoms of natural persons. As outlined above at paragraphs 50 - 97, the security measures that the Commissioner considers Advanced should have implemented were fundamental. The lack of effective vulnerability scanning had been drawn to AHC's attention [redacted]

[redacted] and the ZeroLogon vulnerability had been publicised at least two years prior to the Incident. These factors each increase the responsibility of AHC.

133. The Commissioner notes that Advanced accepts that AHC (as the processor) was responsible for the security of the systems impacted by the Incident.[67] Furthermore, Advanced accepts that decision making regarding the affected IT infrastructure *"sits with AHC (which itself sits within the Health and Care division of the Advanced Group)."* [68]

134. The Commissioner notes that, as per Advanced's Master Agreement with its controller customer entities, the data controller customer entities will also need to take appropriate security measures to protect their personal data. However, the Commissioner does not consider this reduces AHC responsibility as a data processor to have in place appropriate technical and organisational measures in accordance with Article 32 UK GDPR.

135. The Commissioner considers that Advanced's size, experience in personal data processing and the volume and nature of personal data it processed, means that it has a higher degree of responsibility for these basic security failings given higher standards of security are expected of it than would be expected of a much smaller organisation.

136. The Commissioner considers Advanced's degree of responsibility to be an aggravating factor.

Relevant aggravating or mitigating factors: Article 83(2)(e) any relevant previous infringements by the controller or processor

[67] Letter from Norton Rose Fullbright to ICO dated 4 February 2023
[68] Letter from Norton Rose Fullbright to ICO dated 4 February 2023

137. The Commissioner is not aware of any relevant previous infringement. This factor is therefore not relevant to his decision.

Relevant aggravating or mitigating factors: Article 83(2)(f) the degree of cooperation with the Commissioner

138. Controllers and processors are expected to cooperate with the Commissioner in the performance of the Commissioner's tasks, for example by responding to requests for information and attending meetings. The Commissioner considers that the ordinary duty of cooperation is required by law and meeting this standard is therefore not a mitigating factor.

139. Advanced has responded to requests for information during the Commissioner's investigation. In doing so, the Commissioner's view is that Advanced has demonstrated the expected level of cooperation. Therefore, the Commissioner considers this to be a neutral, rather than mitigating, factor. Advanced's settlement with the Commissioner is reflected in a specific discount at a separate step and therefore is not included as a mitigating factor.

Relevant aggravating or mitigating factors: Article 83(2)(h) the manner in which the infringement became known to the Commissioner

140. The infringement became known to the Commissioner as a result of news reports regarding outages to healthcare services on 5 August 2022.

141. There is no obligation on the data processor to notify the Commissioner of a suspected data breach. This factor is therefore not relevant to the Commissioner's decision.

Relevant aggravating or mitigating factors: Article 83(2)(i) measures previously ordered against the controller or processor

142. There are no measures referred to in Article 58(2) UK GDPR which have previously been ordered against Advanced. This factor is therefore not relevant to the Commissioner's decision.

Relevant aggravating or mitigating factors: Article 83(2)(j) adherence to approved codes of conduct or certification mechanisms

143. There are no relevant codes of conduct or approved certification mechanisms. This factor is therefore not relevant to the Commissioner's decision.

Relevant aggravating or mitigating factors: Article 83(2)(k) any other applicable aggravating or mitigating factors

144. The Commissioner has considered whether Advanced benefited from any financial gain in not implementing the required security. The Commissioner considered that some savings were likely to have been made, however, the Commissioner believes such savings were unlikely to have been significant and therefore has not taken them into account.

145. The Commissioner may also consider any action Advanced took to pro-actively report the cyber security breach to other appropriate bodies (such as the NCSC). In representations dated 23 September 2024, Advanced confirmed that it proactively reported to the NCSC and the NCA shortly after discovering the incident. The Commissioner therefore considers this to be a mitigating factor.

Conclusion on relevant aggravating and mitigating factors

146. The Commissioner has considered the degree of Advanced's responsibility as an aggravating factor.

147. The Commissioner has taken into account the steps taken by Advanced to mitigate the mitigate the damage suffered by the data subjects, and the steps taken by Advanced to proactively notify and work with the NCSC and NCA, as mitigating factors.

148. However, these mitigating factors do not outweigh the seriousness of the infringement and therefore the Commissioner considers that a penalty remains appropriate.

149. The final stage involves consideration of the effectiveness, proportionality, and dissuasiveness of a penalty.

Effectiveness, proportionality, and dissuasiveness

150. The Commissioner considers the imposition of a penalty would be effective, dissuasive, and proportionate. It would promote compliance with data protection legislation and provide an appropriate sanction for the infringement.

151. Taking into account the high degree of seriousness of the infringement, the size of Advanced and its financial position, the Commissioner considers that the imposition of a penalty would be proportionate. It would not exceed what is appropriate and necessary in the circumstances to ensure compliance with data protection legislation and to provide an appropriate sanction for the infringement.

152. AHC will continue to process personal data on behalf of data controllers so there is a need for specific deterrence. There is also a

need to deter other data controllers and processors from committing infringements of the UK GDPR.

153. The Commissioner considers that the penalty will raise awareness of the need for data controllers and processors to ensure that they have appropriate technical and organisational security measures in place.

Deregulation Act 2015

154. In making his decision, the Commissioner has also had regard to the factors set out in s108(2)(b) of the Deregulation Act 2015; including: the nature and level of risks associated with non-compliance, including the risks to economic growth; the steps taken by the business to achieve compliance and reasons for its failure; the willingness and ability of the business to address non-compliance; the likely impact of the proposed intervention on the business, and the likely impact of the proposed intervention on the wider business community, both in terms of deterring non-compliance and economic benefits to legitimate businesses.

155. Having considered the factors set out in s108(2)(b) against the matters set out in this notice, and with regard to Advanced's position as a UK based enterprise, the Commissioner, the Commissioner considers the Notice is unlikely to have an impact on any measure of economic activity or growth in the UK, including employment and GDP.

C. Conclusion on decision on whether to impose a penalty

156. In light of the above, the Commissioner decides to impose a penalty.

VI. CALCULATION OF PROPOSED PENALTY

157. The Fining Guidance sets out a five-step approach which the Commissioner proposes to apply to calculate the amount of a penalty:

Step 1: Assessment of the seriousness of the infringement.

Step 2: Accounting for turnover (where the controller or processor is part of an undertaking).

Step 3: Calculation of the starting point having regard to the seriousness of the infringement and, where relevant, the turnover of the undertaking.

Step 4: Adjustment to take into account any aggravating or mitigating factors.

Step 5: Assessment of whether the fine is effective, proportionate, and dissuasive.

158. Whilst the Commissioner has applied this approach, the overall assessment of the appropriate fine amount involves evaluation and judgment taking into account all the relevant circumstances of the individual case.

Statutory maximum penalty

159. An infringement of Article 32(1) UK GDPR is subject to the standard maximum statutory penalty of £8.7m, or in the case of an undertaking, 2% of the worldwide annual turnover of the preceding financial year, whichever is higher (Article 83(4)(a) UK GDPR).

160. The Fining Guidance considers the concept of an undertaking for the purpose of imposing fines at paragraphs 23 – 31. Where a controller or processor forms part of an undertaking, the Commissioner will calculate the maximum fine based on the turnover of the undertaking

as a whole. Whether or not an individual controller or processor forms part of a wider undertaking depends on whether it can act autonomously or whether another legal or natural person, for example a parent company, exercises decisive influence over it.

161. Paragraph 30 of the Fining Guidance[69] states:

"Where a parent company owns all, or nearly all, the voting shares in a subsidiary there is a presumption that the parent company exercises decisive influence over the subsidiary's conduct. This presumption may be rebutted. However, the burden is on the parent company to provide sufficient evidence to demonstrate that the subsidiary acts independently."

162. The relevant legal entity impacted by the Incident was AHC. AHC is ultimately wholly owned by Aston. The Commissioner can rely upon the presumption that the parent company, Aston, exercises decisive influence over its wholly owned subsidiary, ACSG. Furthermore, the Commissioner can rely on the presumption that ACSG, in turn, exercised decisive influence over its wholly owned subsidiary, AHC. Advanced submitted in representations that it considered AHC to be the appropriate undertaking in the context of the Incident as it was the part of Advanced that was directly impacted by the Incident. The Commissioner gave very careful consideration to the submissions and determined on the basis of the evidence overall that ACSG had the ability to and actually exercised decisive influence over the conduct of AHC.

[69] Paragraph 30, of the Fining Guidance data-protection-fining-guidance-0-1.pdf (ico.org.uk).

163. The Commissioner is therefore entitled to calculate the maximum fine based on the turnover of the Advanced Group as a whole (being that disclosed in the accounts of Aston) and use the same turnover when determining any adjustment to be made at steps 2 and 3 of the calculations laid out in the Fining Guidance.

164. On 3 July 2024, Advanced provided the financial accounts of Aston for the financial year ending 29 February 2024 which demonstrate a reported revenue of £323.8 million. 2% of this figure is £6,476,000 which is less than the standard maximum penalty of £8.7 million.

165. In this case, the calculation of the penalty will proceed based on the single statutory maximum of £8.7 million.

A. Step 1: Assessment of the seriousness of the infringement

166. As set out at paragraphs 109 to 115 of the Fining Guidance, the Commissioner determines a starting point for the penalty first by assessing the seriousness of the infringement. The Commissioner categorises the infringement according to its degree of seriousness and then choses a starting point based on a percentage of the relevant applicable statutory maximum.

167. In the NOI, the Commissioner provisionally categorised the infringement as having a high degree of seriousness. Having carefully considered Advanced's representations, the Commissioner continues to categorise the infringement as having a high degree of seriousness. This means that the starting point will be between 20% and 100% of the relevant legal maximum (£8.7 million).

168. In the NOI, the Commissioner provisionally decided that the infringement warranted a starting point of 70% due to the seriousness of the infringement, the sensitive nature of the personal

data being processed, the extent of the processing and number of data subjects and the fundamental nature of the security failings concerned.

169. Having reflected on Advanced's representations regarding the seriousness of the infringement, the Commissioner determines that the appropriate starting point is 65%. This is on the basis that, whilst there was an impact on the provision of healthcare services following the Incident, there is no evidence of actual harm to data subjects. There was also a slight reduction in the number of data subjects impacted, and 38,208 data subjects out of the 79,404 had no special category data impacted.

170. In adjusting the starting point, the Commissioner has also considered Advanced's representations that, at the time of the incident, MFA was in place for Adastra and Carenotes, although in the circumstances of this incident, this was ineffective as the Threat Actor was still able to access the AHC domain as MFA had not been rolled out to all AHC products. The Commissioner's full assessment of seriousness is set out at paragraphs 103 to 127 above.

B. Step 2: Accounting for turnover

171. Having assessed the seriousness of the infringement, the Commissioner next determines any adjustments to account for turnover as set out in paragraphs 116 to 129 of the Fining Guidance. This step permits the Commissioner to adjust the starting point to reflect the size of the undertaking.

172. Aston's turnover for the year ending 29 February 2024 was £323.8 million. This means that the range of adjustment based on the

turnover of the undertaking will be between 50% and 100%.[70] Paragraph 128 of the Fining Guidance states that the Commissioner must decide whether it is appropriate to adjust the starting point on a case-by-case basis, and the Commissioner retains the discretion to impose a fine up to the applicable statutory maximum.

173. In the NOI, the Commissioner provisionally considered that it was appropriate to make no adjustment to the starting point to reflect the size of the undertaking having regard to the need for the fine to be effective, proportionate, and dissuasive. In reaching this view, the Commissioner took into account the Advanced Group's financial position, the fact that the penalty would encourage Advanced's compliance with data protection law, and the need for the penalty to act as a deterrent to other data processors in a similar position to Advanced.

174. In the representations dated 23 September 2024, Advanced submitted that the Commissioner's approach at this step was a misapplication of the Fining Guidance and manifestly unfair. Advanced submitted that the range within Table B of the Fining Guidance should be treated as a sliding scale and therefore the starting point for the penalty should be adjusted by 71%.

175. The Commissioner considers that an adjustment at Step 2 is not automatic and needs to be considered on a case-by-case basis having regard to the need for the fine to be effective, proportionate and dissuasive, as per the Fining Guidance. The Commissioner retains the discretion to consider financial performance of a data controller and/or processor, the circumstances of the infringements and the need for the fine to be effective, proportionate and dissuasive when

[70] Fining Guidance – Table B: Ranges for adjustment based on the turnover of the undertaking.

deciding what adjustment, if any, to make at this stage. Furthermore, if an adjustment is to be made, the ranges in Table B are indicative. The Commissioner therefore does not accept Advanced's submissions that its approach in the NOI was manifestly unfair and/or legally flawed.

176. Notwithstanding the above, and having considered Advanced's representations, the Commissioner considers it would be appropriate to make an adjustment of 80% to account for turnover. This adjustment would be proportionate taking into account the fact that Advanced Group's turnover does fall within the range where an adjustment is permitted and the fact that the infringement only concerned the AHC environment as opposed to the entirety of the Advanced IT network, but also the need for the penalty to be effective and dissuasive.

C. Step 3: Calculation of the starting point

177. The starting point for the penalty is calculated as follows: Fixed statutory maximum amount (£8.7 million) x adjustment for seriousness (65%) x turnover adjustment (80%) = **£4,524,000**.

D. Step 4: Adjustment to take into account any aggravating or mitigating factors

178. The Commissioner next takes into account any aggravating or mitigating factors. These factors may warrant an increase or decrease in the penalty calculated at the end of Step 3 (the starting point of £4,524,000).

179. In the NOI, the Commissioner provisionally decided not to make any adjustment to account for aggravating or mitigating factors. Having carefully considered Advanced's representations the Commissioner

has decided to adjust the penalty to account for mitigating factors by reducing the penalty by **15%.** This reflects the steps Advanced undertook to mitigate the impact to data subjects (listed at paragraph 114 to 117 above) and Advanced proactively reporting the matter to the NCSC and NCA.

180. The Commissioner makes no adjustment for the aggravating factors listed at paragraphs 131 - 136 which have been adequately reflected as part of the seriousness assessment at Step 1.

181. The penalty at Step 4 is **£3,845,400**

E. Step 5: Adjustment to ensure the fine is effective, proportionate and dissuasive

182. As set out in the Fining Guidance, "*the aim of Steps 1 to 4 of the calculation is to identify a fine amount that is effective, proportionate and dissuasive. The purpose of Step 5 is to provide the opportunity for the Commissioner to check that is the case.*"

183. The Commissioner considers that a penalty of £3,845,400 will be effective and dissuasive. A penalty in this amount will have a genuine deterrent effect, taking into account both the specific deterrent to Advanced and the general deterrence to other organisations.

184. The penalty is specific to the nature of the infringement, particularly when set in the context of the sensitive nature of the personal data Advanced was processing on behalf of the data controller customer entities, and the disruption the infringement had on healthcare services after the Incident. The penalty is also proportionate when taking into consideration that the infringement relates to failings in cyber security measures which could have been rectified. The

Commissioner notes that these measures were in place in Advanced's corporate setting but not fully deployed in the AHC environment where the Incident took place.

185. The penalty also reflects Advanced's financial position. The penalty is not more than is appropriate or necessary in the circumstances.

186. In considering the penalty, the Commissioner has also taken into account fines placed in similar cases.[71] Taking into account the individual circumstances of these cases, in comparison with the circumstances of the infringement against Advanced, the Commissioner considers the penalty of £3,845,400 to be proportionate.

187. The penalty of £3,845,400 does not exceed the statutory maximum.

F. Settlement

188. As set out at paragraph 5 above, Advanced has acknowledged the Commissioner's decision in this Penalty Notice. In light of this acknowledgement and Advanced's agreement not to appeal against this Penalty Notice, the Commissioner has reduced the penalty by 20%.

189. This reduction is applied to recognise that Advanced's cooperation has allowed the Commissioner to make time and cost savings (both in the procedure to date and going forward) and achieves regulatory certainty sooner by avoiding an appeal.

---

[71] INTERSERVE GROUP LIMITED monetary penalty notice (ico.org.uk) – 19 October 2022, £4.4 million, Marriott International Inc, Penalty Notice – 30 October 2020 (ico.org.uk) - £18.4 million
British Airways Penalty Notice - 16 October 2016 (ico.org.uk) - £20 million

190. A reduction of 20% to the penalty of £3,845,400 gives a final penalty of £3,076,320.

G. Conclusion – Penalty

191. For the reasons set out above, the Commissioner has decided to impose an administrative penalty on Advanced Computer Software Group Limited, Advanced Health and Care Limited and Aston Midco Limited in the amount of **£3,076,320**.

VII. FINANCIAL HARDSHIP

192. The Fining Guidance outlines that, in exceptional circumstances, the Commissioner may reduce a fine where an organisation is unable to pay due to its financial position. Advanced has chosen not to make any representations regarding financial hardship.

VIII. PAYMENT OF PENALTY

193. The penalty must be paid to the Commissioner's office by BACS transfer or cheque by either 30 April 2025, or paid in accordance with an agreed payment plan.

194. The Commissioner will not take action to enforce a penalty unless:

- The period within which a penalty must be paid has expired and all or any of the penalty has not been paid;
- All relevant appeals against the penalty and any variation of it have either been decided or withdrawn; and
- The period for appealing against the penalty and any variation of it has expired.

IX. APPEAL

195. There is a right of appeal to the First-Tier Tribunal (Information Rights) pursuant to s.162 of the DPA against:

    a. The imposition of the penalty; and/or
    b. The amount of the penalty specified in the penalty notice.

196. Any notice of appeal should be received by the Tribunal within 28 days of the date of this Penalty Notice.

197. Advanced has acknowledged the Commissioner's decision to impose a penalty and amount of the penalty and has agreed not to appeal this Penalty Notice.

Dated: 26 March 2025

Stephen Bonner
Deputy Commissioner, Regulatory Supervision
Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF