STEPHENSON HARWOOD

20 October 2025

ICO IMPOSES A £14 MILLION FINE FOR DATA BREACH THAT IMPACTED 325 PENSION SCHEMES

The UK's Information Commissioner's Office ("ICO") has imposed a £14m fine on Capita for a data breach it suffered in March 2023. The breach was suffered after an unknown threat actor gained access to Capita's systems following the inadvertent download of a malicious file onto an employee device, which led ultimately to the theft of the personal data of 6.6 million individuals, including highly sensitive data, such as financial information, criminal record data, data relating to children, and other 'special category' data.

The ICO's press release confirms that 325 pension scheme organisations have been impacted by the breach.

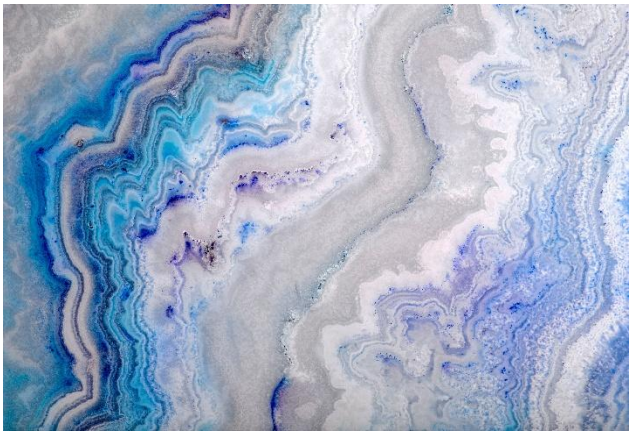
In its penalty notice, the ICO provides commentary on the cyber security measures adopted by Capita, including that it did not act to quarantine the initially-compromised user device quickly enough (the delay was some 58 hours), despite initial automated detection of suspicious activity having occurred almost immediately after the initial file download. The ICO notice records that this delay in acting permitted the threat actor to gain wider access to Capita's systems, including gaining administrator privileges, and allowed them to exfiltrate approximately 1TB of data. The threat actor then deployed ransomware onto Capita's systems and reset user passwords, preventing Capita employees from accessing its systems.

The ICO's findings include that Capita "failed to ensure the security of processing of personal data" and was "lacking the appropriate technical and organisational measures to effectively respond to the attack".

The ICO sent an initial notice of intent to Capita in April 2025, in which it stated its intention to impose a £45m fine. Capita made representations to the ICO, including submitting mitigating factors, and a voluntary settlement was agreed with a reduced fine of £14m. Capita has accepted liability, acknowledged the ICO's decision, and has agreed not to appeal.

In setting out its final decision, the ICO identified several proactive steps which it says organisations in general should be taking to reduce security risks, including:

- following guidance issued by the National Cyber Security Centre on preventing "lateral movement" by threat actors within the organisation's systems and networks – a crucial step in limiting the damage that can be done even if an attacker is initially successful in gaining unauthorised access to a particular device or component of the system;
- regularly monitoring for suspicious activity and responding to initial warnings and alerts in a timely manner;
- sharing the findings from penetration testing across the whole organisation so that risks can be universally addressed;
- prioritising investment in key security controls to ensure that they are operating effectively; and
- ensuring that agreements and responsibilities between data controllers and data processors are well understood by all stakeholders.



Given the scale and impact of this incident across the pensions industry, as well as the increasing frequency and sophistication of cyber-attacks more generally – including the growing risk posed by supply chain attacks – organisations in the pensions sector are advised to review and refresh their cyber policies and procedures. Our cyber and data protection team is well-versed in providing rapid, strategic support at every stage of the cyber life cycle – please do reach out if you'd like to discuss any aspect further.

CONTACT US

STEPHEN RICHARDS
Partner, Pensions

+ 44 20 7809 2350
stephen.richards
@stephensonharwood.com

ESTELLA BOGIRA
Partner, Pensions

+ 44 20 7809 2298
estella.bogira
@stephensonharwood.com

JOANNE ELIELI
Partner, IP Tech & Data

+ 44 20 7809 2594
joanne.elieli
@stephensonharwood.com

PHILIP GOODCHILD
Partner

+ 44 20 7809 2166
philip.goodchild
@stephensonharwood.com