The Pensions Regulator

Capita cyber security incident

Published: 12 May 2023.

Capita has recently experienced a cyber security incident and it is now known that some data has been exfiltrated from their servers.

As trustees, you are responsible for the security of your members' data. If you use Capita's services, you should check whether your pension scheme's data could be affected. Make sure you keep communicating with Capita as the situation evolves.

This situation is likely to cause concern to members and you should be prepared to answer their queries. You should contact your members proactively to warn them about pension scams (/en/trustees/communicate-to-members/warn-members-about-pension-scams) and keep them updated while you confirm whether a data breach has taken place. You should also monitor increased or unusual transfer requests (/en/document-library/scheme-management-detailed-guidance/administration-detailed-guidance/dealing-with-transfer-requests) .

If there has been a data breach in your scheme, you may need to notify affected individuals and should direct them to data breaches guidance for individuals from the National Cyber Security Centre (https://www.ncsc.gov.uk/guidance/data-breaches) . You may also need to notify us (/en/document-library/codes-of-practice/code-1-reporting-breaches-of-the-law) and the Information Commissioner's Office (https://ico.org.uk/for-organisations/report-a-breach) .

This incident shows the importance of having a robust cyber security and business continuity plan in place. Make sure you have read our cyber security guidance (/en/document-library/scheme-management-detailed-guidance/administration-detailed-guidance/cyber-security-principles) and check that your own plans are up to date.

We may engage with you further to understand the steps you have taken and what progress you have made.