Capita Cyber Incident

Questions and answers

We updated this Q&A on 09 October 2024. We have made it specific to the incident and post incident activity and included updated information on the most frequently asked questions.

The information about the Experian service is now updated in a separate Q&A which can also be found on the online cyber hub at **www.eapf.org.uk/cyber**.

1. How and when did the cyber incident at Capita occur?

The cyber incident occurred at Capita plc, and it impacted a small number of its computer servers. This included some used by Capita Pension Solutions, which is a business that provides pension administration services to members of the Environment Agency Pension Fund (EAPF), along with other major pension schemes.

The initial malicious activity took place on 22 March 2023. Capita detected the activity on 31 March 2023 and intercepted it immediately.

2. What action has Capita taken since the incident?

Capita then undertook a complex forensic investigation with support from technical experts and specialist advisers. This involved reviewing files across their entire business.

Capita has taken extensive steps to recover and secure the data contained within the impacted server estate, and to remediate any issues arising from the incident.

Capita appointed a third-party specialist adviser who continues to monitor the dark web to confirm that data exfiltrated as a result of this incident is not being circulated or available for sale online. Capita's specialist advisers have been appointed since the earliest days of this cyber incident. Capita do not have any evidence that any of the exfiltrated data is circulating on the dark web, or that it is available for sale online or otherwise. More detail on the dark web and what this means in practice is included in question 7.

- Since the incident, Capita has taken further steps to ensure the integrity, safety and security of its IT infrastructure to underpin its ongoing client service commitments. Capita has undertaken several initiatives to ensure that their internal IT infrastructure, processes and procedures remain compliant with all legislative and regulatory requirements for data security. Recognising the limits of how much can be publicly shared on this, Capita have stated that these initiatives include:

    - A technical report covering the tactical recovery of certain aspects of the IT infrastructure, and causes of the incident, using an external technical expert. Capita's position is that the report provided the necessary assurances at this point on the areas reviewed.

    - Following the cyber incident, Capita wrote to any impacted members with details of what data items had been exfiltrated along with recommended steps to help protect you from the risks posed by cyber-attacks such as the one experienced by Capita. To provide an additional level of assurance, Capita has engaged a reputable independent third-party organisation to audit the

results of the analysis they conducted. This will make sure that no member or data item has been missed from Capita's analysis. It was anticipated that this audit would be completed during autumn 2023, but the complexity of it has delayed completion. Capita anticipate providing us with an update for the Pension Fund within the coming months. Nothing of concern has been identified for the Pension Fund at this point. Should there be any difference to the results, we will inform any impacted members as soon as possible.

3. Why can't you tell us more about the reports that have been completed to investigate whether Capita had sufficient measures in place to avoid the incident?

We are limited in what we can say about Capita's cyber incident and Capita's IT infrastructure and internal processes. We signed a non-disclosure agreement (NDA) with Capita soon after the incident to ensure we could access certain confidential information quickly to assess the impact, and this unfortunately precludes us from disclosing the confidential information received from Capita.

4. Have any investigations been completed that you can tell us about?

The Pensions Regulator (TPR) has published its report into the incident on 2 February 2024. This provides some background to the incident and the steps TPR undertook with Capita and Pensions Schemes. It also sets out TPR expectations of Pensions Schemes and Trustees on cyber security. Updated cyber guidance was published by the TPR in December 2023.

Read the TPR report published on 2 February 2024.

5. What are your legal and regulatory obligations?

We are required to inform the Information Commissioners Office (ICO) and the Pensions Regulator (TPR) about the incident. We have reported the impact to the Fund to both ICO and TPR in the early stages and have continued to work with them on their investigations.

6. Is there any guidance available from a regulatory perspective?

The National Cyber Security Centre and the ICO both provide guidance that may also be useful. You can visit their websites using the below web addresses:

www.ncsc.gov.uk/guidance/data-breaches

ico.org.uk/for-the-public

7. How will you make sure that this doesn't happen again?

The Pension Fund takes the protection of members' data very seriously. We have undertaken cyber security assessments, audits and training across the Pension Fund and key external providers (including Capita) both prior to and since this incident. We use advice from internal and external experts to ensure we meet all regulatory requirements and guidance (such as the TPR guidance).

Since the incident, Capita has taken further steps to ensure the integrity, safety and security of its IT infrastructure to underpin its ongoing client service commitments. Capita has undertaken several initiatives to ensure that their internal IT infrastructure, processes and procedures remain compliant with all legislative and regulatory requirements for data

security. Recognising the limits of how much can be publicly shared on this, we have included an update on Capita actions under question 2 above.

We understand the importance of providing assurance for our members and will update further on this as soon as we are able to do so.

8. What is the latest position on the Information Commissioners Office (ICO) investigation? Why is it taking so long?

The Environment Agency's data security team were required to report the breach to the ICO (separately to Capita' own report of the breach to the ICO). This is to ascertain whether in the capacity as the 'data controller' the necessary steps were taken to ensure the data is adequately protected. The Environment Agency received confirmation on 3 February 2024 that the investigation into this aspect is complete and that there is no further action.

We understand that other organisations also impacted by Capita's data breach have received the same update.

Capita continue to work collaboratively with the ICO, and at this time, the ICO have not provided Capita with a timescale for completion of their enquiries. We do not know when any report or decision on this may be made but we will update you when we have this information.

It may be helpful to note that other for organisations who have experienced a Cyber attack in recent years, it is not uncommon for these enquiries to take quite some time before a determination is made.

The ICO are also required to publish the outcome of their enquiries at the time they are available.

9. Have members been notified what personal data was exfiltrated in the incident?

All impacted EAPF members and former members have been written to. All letters include the relevant information setting out the precise categories of personal data impacted, as well as an activation code for 24 months complimentary membership to a trusted identity protection service from Experian.

Whilst Capita has informed us that there is no evidence that information resulting from this incident has been misused (please see more about this in question 12 below), Capita believes it is appropriate to act with vigilance under the circumstances.

10. What does 'exfiltrated' mean in the context of this incident?

The definition of 'exfiltrated' in a cyber security context is:

- The unauthorised transfer of information from an information system

11. What could someone do with my data if it is sold online? What are the risks to me?

It's important to note that to date, it remains the case that there is no evidence that the data has been sold or leaked on the dark web, which Capita are continuing to monitor closely through third party experts. Capita have set out that the risk is the potential for identity fraud in the event that data is misused.

Identity fraud could take the form of: trying to open an account in someone's name/ making a purchase in someone's name/using someone's personal details in criminal activity such as

using fake details for car insurance, etc.

In order to reduce the risk to members, they recommend using the Experian service in addition to vigilance in the form of looking out for suspicious emails and using caution in clicking on links without verifying it's from a reliable source.

12. What exactly is the third-party monitoring looking for? Why are you telling us there is no signs of the data when I've had an Experian notification saying my details have been found on the web?

Capita appointed the third-party experts who have been monitoring the dark web on a daily basis since the earliest days of the incident, looking for evidence of matches to the exfiltrated data. To date, no evidence has been found matching the Capita data that was breached in the attack.

The dark web is a part of the internet that is hidden from public search engines and can only be accessed by using special software. The specialist team who are providing this monitoring, use a tool that can access the dark web. The software they use scans the dark web specifically for matches to the Capita data that was included in the exfiltrated data.

As there's still no evidence of this, in Capita's view any fraudulent activity picked up to date isn't therefore linked to the cyber attack. With the Experian membership in place, they believe members are also now that much more aware of any unusual activity, which can only be a good thing.

The Experian service monitors the data that a registered member shares with them, it is therefore not specific to the data exfiltrated as part of the Capita cyber incident. It is also completely separate to the third party expert monitoring. Experian looks for evidence of the information they have for registered members using the verified information on their profile, and anything additional that individuals choose to be monitored.
For example, a member might have shared other email accounts that were not included in the Capita data breach, or financial information that wasn't included too. Some members have reported to us that they have received Experian alerts and have assumed that this is part of the data breach.

Unfortunately, the digital era we live in has seen a significant increase in criminal cyber attacks in recent times. Many of these attacks go unreported to the victims whose data has been breached. We do believe that having the Experian service available is key to increased awareness of when details are found – making it possible for those receiving the alerts to take action when this is the case.

Any alerts through the Experian service will include the data item that has been found on the web, but it will not confirm the date this data first appeared on the web – which could go back up to 6 years prior to registering with the Experian service.

The alert may ask some questions to confirm whether the member recognises it and will give some recommended steps they should take to keep their details safe – such as changing passwords, or contacting them for something of greater concern.

Both Capita and Experian advise that the steps set out are the best way to protect members who receive these alerts.

It's also been a common cause of concern where members have previously used a comparison service for financial services such as insurance. Many of these sites will perform

a search automatically in the lead up to the anniversary of the renewal date. Often, this will create multiple notifications on the Experian service – which can cause concern for members who don't recognise that they have applied for anything. However, where this is the case, it's often explained by an upcoming renewal for any form of insurance previously taken out.

13. How long will the third-party expert continue monitoring the dark web for signs of my data being sold or misused?

Capita's agreement for this monitoring is open with no cessation date planned.

14. What happens when my 24 month Experian membership comes to an end? Will you extend it?

There are no plans to extend the Experian membership beyond 24 months. This is because the third-party daily monitoring service appointed by Capita has not identified any evidence of the exfiltrated data appearing on the dark web to date. This has reassured us that the extension of the Experian service is not necessary to continue beyond the 24 months provided.

Capita's appointed third party monitoring service will continue with no planned date for this to end. If anything changes in terms of evidence being found, we may look to review the Experian offering in that situation.

Whilst it may be comforting to have Experian as an additional personal check, it is the individual member's choice as to whether they wish to continue with the identity plus Experian monitoring at their own cost. Experian offer different levels of monitoring. More information about the options available can be found on the Experian website at **www.experian.co.uk/consumer/which-product-is-right-for-me.html**:

15. I've noticed an increase in spam texts and phone calls too since the cyber incident, are these linked to the breach?

Phone numbers were not included in the exfiltrated Capita data. Therefore, this cannot be linked to the cyber breach. As explained in question 12 above, there are commonly breaches that go unreported and so any increase in spam texts or calls may be linked to something separate.

16. Is my pension safe?

We'd like to reassure all members that your pension benefits remain secure. Hartlink, the database that holds all member pension records, was not impacted by this incident. The main advice we can provide is not to be alarmed, but to be vigilant given the circumstances.

We have set out some recommendations in question 18 below.

17. Could somebody contact Capita posing as me and change my bank details? (For a pensioner member)

We have confirmed this with Capita and are satisfied that they have robust identity and verification procedures to be assured an individual making contact is indeed a member of the EAPF. Changes to the personal details Capita currently holds about you require additional evidence to be provided to verify any change.

For bank changes – these are not accepted over the phone because of the security risk this poses – and evidence of the change must be provided.

From the assurances and procedures outlined by Capita to us, it is clear that it would be very unlikely that bank details could be changed by anyone other than our members.

18. What advice can you give to members who are concerned?

Whether you've been impacted by this incident or not, in a data-driven world, we always recommend that members take steps to protect their personal data and avoid scams. We'd encourage all members to only ever give out personal information if you're absolutely sure you know who you're communicating with.

- **If you receive an email from the EAPF administration team**, please make sure the email is from a Capita email address (either @capita.com or @capita.co.uk).
- **If you receive an email from our Communications team**, please make sure the email is from **noreply@mail.eapf.org.uk**
- **If you receive an email directly from our EAPF Management team**, please make sure the email is from **@environment-agency.gov.uk**
- **Use your mouse to hover above an incoming email address to check its origin**, if the email is from a third party pretending to be someone else, you might spot this by holding the mouse above the email address. If anything looks unusual (perhaps a spelling discrepancy or uses numbers in place of letters), it's best to verify the email address through the organisation's website.
- **Do not click on any links included in emails** unless you know it is from a reliable source.
- **Do not provide any personal information** unless it is a request from the administration team that is in direct response to an enquiry from you.
- **If you receive a suspicious email**, you should forward it to **report@phishing.gov.uk** For text messages and telephone calls, forward the information to 7726 (free of charge). For items via post, contact the business concerned.
- **If suspicious emails are received to your work email address,** these should be reported to internal security teams in line with the organisation's policy. For EA, these emails should be reported to **security.team@defra.gov.uk** or for NRW employees, report to **ict.servicedesk@naturalresourceswales.gov.uk**
- If there are any changes to your National Insurance information, HM Revenue & Customs would contact you – but you can also phone them on 0300 200 3500

If you're concerned someone might be impersonating EAPF, please let us know by emailing **info@eapf.org.uk**

19. Is my pension account on the EAPF Portal safe?

Yes, the portal was not accessed, and your login information remains safe.

20. Will Capita give me compensation for the distress the incident has caused me?

We understand that Capita is not paying any voluntary compensation to impacted members as a result of this criminal activity. We do not envisage the Capita position will change at this point.

We understand that, under the UK GDPR, Capita would be legally liable to pay compensation to members if it were established that: (a) Capita had failed to implement appropriate technical and organisational measures to safeguard personal

data (or otherwise breached data protection laws) and (b) this failure had caused members to suffer damage (including distress).

Therefore, it is possible that any members that have suffered distress or other damage as a result of the data breach may have a legal claim to compensation against Capita under data protection law.

As the EAPF is one of many pension funds that have been impacted by this incident, we are also in continuous discussions with other impacted pension funds. In these discussions, ensuring the right support for members is the top priority.

Separately, the data incident has been reported to both the ICO and TPR. As to the regulatory investigation, see questions 5 - 8 above.

If you wish to complain to Capita directly about the incident, you can send an email to **info@eapf.org.uk**.

21. Should I join the 'Class Action' claim against Capita for compensation?

Whilst we continue to correspond with Capita on the issue of compensation on behalf of our members, we understand that a large number of pension holders have already issued a legal claim against Capita. Further information about the legal claim can be found at **www.computerweekly.com/news/366566652/Victims-of-2023-Capita-data-breaches-head-to-High-Court**

It is an individual member's choice whether to join this separate legal claim (which the EAPF is not involved with). We continue to protect the Fund and our members as outlined in question 7.

22. What factors should I take into account when considering whether to join the 'Class Action' claim against Capita for compensation?

Whilst not exhaustive, we have set out below some factors which you may wish to consider when deciding whether to proceed with legal claims against Capita (whether through joining a 'Class Action' claim or otherwise).

Prospects of success – Before committing yourself to proceeding with legal claims, it's important to fully understand the prospects of success for your claim, as well as having a realistic expectation of the damages which you might recover. Please note that in order to recover any sums of money, you'd need to prove that you have suffered actual damage, whether financial or in the form of distress. We note that some claimant law firms tend to advertise based on sums which are likely to be significantly higher than what might actually be recoverable (by the majority of impacted individuals).

Costs –Consider carefully the legal costs which might be payable by you in litigation:

- In relation to your own legal costs, claimant solicitor firms may offer to act on a 'no win, no fee', conditional fee agreement (CFA), or a similar basis. You should carefully read any such terms, in particular, in relation to any "success fees" which may be payable, and the conditions imposed on your ability to remove yourself from the litigation (if you decided that you did not wish to proceed at some point in the future). For example, some CFA terms may restrict your ability to exit the litigation, by requiring you to pay the legal fees and expenses incurred to date on a full fee basis (upon exit).

- In addition to your own legal costs, if the litigation outcome is unsuccessful, claimants could find themselves jointly liable for all of a defendant's costs (as opposed to just their share of the same). You should therefore consider the funding arrangements of the legal action very carefully, including whether insurance has been taken out (to cover the potential costs liability in the event of an unsuccessful claim).

Control – As a member of a 'class action', you will likely have limited control over the litigation process, as the legal team typically makes decisions on behalf of all claimants. This means that decisions might be taken that you may not agree with.

Time – Litigation isn't a quick process. In most instances, cases take many years to progress through the courts. Additionally, if any party were to appeal the court's decision, this would further increase the duration of the claim. Therefore, prior to taking the decision to pursue claims you should be mindful that it's likely you'd be involved in the litigation process for a significant period of time.

Uncertainty – There is no certainty that the outcome of any litigation will be successful and even if a claim is successful, the compensation awarded to you may be lower than you anticipate.

23. What if I have other questions not covered here?

We have done our best to cover as many questions as possible. We have also updated these questions on 8 October following further queries raised since the incident was communicated with affected members.

We'd recommend contacting Experian if you have any questions linked with the Experian service. You can find out more about the Experian service within the separate Experian Q&A in the cyber hub at **www.eapf.org.uk/cyber**.

For other questions that you may have, you can contact Capita at **info@eapf.org.uk** or for anything linked to the management of your pension, you can contact the EAPF management team at **EAPF@environment-agency.org.uk**