Capita Cyber Incident

Questions and answers

You'll be aware that Capita provide the administration services for EAPF members pensions. On 31 March 2023, Capita detected malicious activity on their networks and we have set out below some questions you might have about what this means for our members.

1) How did the cyber incident 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 EAPF, along with several other major pension schemes.

2) When did it happen?

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

Since then, Capita have undertaken a complex forensic investigation with support from technical experts and specialist advisers. This has involved reviewing files across their entire business.

3) When were you first made aware that member data had been affected?

We've been working closely with Capita since it first announced the cyber incident and have sought regular updates on the progress of its investigation. Once Capita had confirmed there was evidence that some personal data may have been accessed, we updated members on the EAPF public website. At this point, they were unable to confirm whether members' personal data had been affected.

We were formally informed of a personal data breach for certain pensioner members in the Scheme late in the afternoon on Friday 19 May. At this point, the full forensic analysis was not complete.

Nevertheless, we updated the website during the following weeks before being in a position to write out to those we believed to be affected in early June. Before the letters were sent, we emailed these members (where email addresses were available), to inform them of the breach and that a letter would follow. Large mailings take time and planning and we had to ensure all our messages were clear and timely.

We've since received the full, final forensic investigation results which confirms the data that was available for our members. We've worked as quickly as we could to review the data in order to write to all affected members setting out exactly how they have been affected.

4) Why has it taken so long for you to write to me?

The full forensic investigation was completed by Capita and shared with the EAPF in mid-June. There are a lot of steps required to produce a large, printed mailing that provides information specific to each individual. This takes a minimum of 7 working days, and we also wanted to make sure you had additional information in the form of the Q&A.

We felt it was important to line up all the appropriate communications needed both internally and externally. Our communications plan has factored in the timescale for the mailing as well as the timing of messages to ensure both we and Capita would have a better ability to respond to queries considering we are only a small team. Please do bear with us if you have to get in touch.

5) What personal data has been accessed in the incident?

Regrettably, details of EAPF members were held on the Capita servers accessed by the hackers. We've written to those EAPF members who have been impacted, setting out the precise categories of personal data impacted.

Whilst Capita has informed us that there is no evidence that information resulting from this incident has been misused, Capita believes it is appropriate to act with vigilance under the circumstances.

6) 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

7) 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 12 below.

8) Has this affected pension payments made to members?

All pension payments have and will continue to be paid on time.

9) Does this impact all members?

Not all, but we now know that all member types are affected and higher numbers than we were initially informed of. The information potentially accessed does vary for each individual and will be set out in their individual letters.

10) Have you contacted all affected members?

We are writing to all members who have been affected by the incident. We have also updated members internally and via the Fund's website confirming details of the incident.

The letter includes the details of the information that was available on the affected server relating to them. It also highlights the potential risks and the steps the affected members can take to protect their personal data. Capita have also provided free access for 12 months to a service that Experian offers (called 'IdentityWorks Global') that will help members monitor the use of their personal data.

11) Is Capita certain that the personal data found on the files has been accessed?

Capita cannot be certain that the personal data has been accessed. You can read Capita's full statement here at **www.capita.com/news/update-actions-taken-resolve-cyber-incident**

12) 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 the 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 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**

13) Is my pension account on the EAPF Portal safe?

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

14) 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 and will work with them on any investigation they choose to conduct and any recommendations they may make.

15) Should I also contact ICO even though you have?

There is no need for members to contact ICO as they are already aware of the data breach and have been provided with regular updates for the EAPF and Capita.

16) 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

17) Are and how are the unions being involved in this?

The trade unions have been kept informed of the situation and we'll continue to engage with the unions as and when we have an update on the forensic investigation results.

18) How will you make sure that this doesn't happen again?

In our discussions with Capita, we have sought information about what has been done to improve the security of personal data and avoid a future incident. Now that the investigation has been finalised, we are awaiting a full report about the incident, how it was managed and what steps Capita has taken and will be taking to avoid this happening again.

19) The unknown of what and where our data may be used or not, is very stressful and worrying.

We want you to know that your Pensions Committee, plus the Environment Agency Board and Senior Leadership in the organisation are taking this cyber incident very seriously. They are monitoring Capita closely and want to ensure that members are being supported.

It's also important to recognise that this is still a live incident and there is further work required.

20) All of this data should have been segregated and encrypted - was this not the case?

Some of the data was encrypted, but sadly not all. EAPF has written to you because at least some of the information Capita handles on behalf of EAPF was not password protected or encrypted.

We appreciate that this will be a concern to you, and we understand your frustration. We understand that Capita have appointed a third-party specialist adviser who continues to monitor the dark web to confirm that data compromised as a result of this incident is not available for sale online.

Further, Capita have assured us that they are continuing with their multi-year investment programme focused on ensuring the integrity of its cyber-security environment. However, unfortunately, no entity can assure themselves they will never experience a cyber-incident.

21) What service can I use to monitor the use of my personal data?

To help you monitor your personal information for certain signs of potential identity theft, Capita are providing a free 12 month membership through Experian to 'IdentityWorks Global'. A unique voucher code and the steps to register to the service will be included in the letter affected members will receive.

Experian service available to minors under 18

In order to use this service, your parent or guardian can, with your consent, sign up on your behalf. If you'd like more information on this, please speak to Experian on 020 8090 3696.

22) Who are Experian?

Experian are a trusted, leading identity protection service who specialise in the protection of data. This service helps detect possible misuse of your personal data and provides you with identity monitoring support, focused on the identification and resolution of identity theft.

23) How does the Experian service work?

Once you've registered, this service notifies you via email or SMS whenever your personal information has been found on the web. You'll then be asked to log into this service where you'll then be presented with a report which explains what information has been found.

24) How can Experian help me to protect myself from fraudulent activity?

As well as the Experian service alerting you via email or SMS if your personal information is found on the web, they also have an education centre which helps you consider the most appropriate steps you could take to protect yourself. This vital insight can help you to determine if you're at risk and to help reduce the risk of becoming a victim of fraud in the future.

25) What personal information is monitored by the Experian service?

Experian monitors the dark web, to find specified personally identifiable information. For example, your first name, last name, email address, phone number, debit card and credit card number (max of two), driving licence number, passport number, National Insurance number, IBAN (International bank account number).

26) What are the approved countries for IdentityWorks (Global)?

These are the current countries that have been approved for this service:

Australia, Austria, Brazil, Canada, Denmark, Finland, France, Germany, Hong Kong, India, Ireland, Italy, Malaysia, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Singapore, Spain, South Africa, Sweden, Switzerland, Turkey, United Kingdom, United States, Puerto Rico, Guam and US Virgin Islands.

27) How do I register for the Experian service?

Affected members will receive a letter containing a unique voucher code which can be used to register for the free 12 month membership. The letter explains the steps to follow to access this service. There is also a contact number so you can speak directly to Experian if you have any questions.

28) How do I use the Experian service as a minor (under age 18)?

In order to use this service, your parent or guardian can, with your consent, sign up on your behalf. If you'd like more information on this, please speak to Experian on 020 8090 3696.

29) Is 12 months Experian membership enough? The data can be out there forever for criminals to use.

We do appreciate the concern around your data being exfiltrated and the unknowns and uncertainty of what will happen with this in the future. We are in discussion with Capita regarding the service offering with Experian going forwards. However, at this point in time it is too early to know whether or not the 12 month monitoring will be extended.

30) Why should we have to provide another third party with our personal data to access support?

We appreciate the irony in the need to provide personal information to Experian, however this is necessary for them to be able to accurately monitor the situation for you.

It is your choice whether or not you wish to sign up to the Experian service. So, if you don't wish to share your information with another third party supplier then you don't have to.

But Experian are a leading identity protection service who specialise in the protection of data. They provide a trusted facility, which can provide peace of mind that you'll be alerted if you're at threat of becoming a victim of fraud.

31) Will this affect those already receiving, or who are about to receive, state pensions?

No, it will not. Neither your state pension, nor your EAPF pension, were impacted by the incident. The incident will not affect your upcoming, or already received, pensions.

The impact of the incident is limited to the exfiltration of certain data held by Capita in relation to your EAPF pension, so we are making you aware of the situation and recommending you register with Experian and stay vigilant.

32) 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.

33) I've heard that it will cost £15-£20 million for Capita to recover from the incident. Does Capita have insurance to cover this cost so that it will not affect our pension?

Capita have the relevant insurance as you would expect for an organisation of their size. Member pensions are protected in statute. The funds held in EAPF are completely separate and will not be affected by any costs to Capita for the breach. The £15-£20m costs estimated to recover from the incident relate solely to Capita and not the EAPF or any other Capita clients.

34) There are lots of firms touting for business in relation to claiming compensation regarding this data breach with regard to the effect on anxiety etc. What is the EAPF's view of this?

The Fund is liaising with its Legal advisors on a number of issues and will take a view in due course.

35) Are you going to move from Capita following this incident

We procure in line with the guidelines set out by Government. This includes a consideration of how any supplier manages personal data. The process is overseen by Defra Commercial, Independent professional advisors and input from the Pensions Committee.

36) 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 27 June following some useful points raised since our last mailing.

Below are also some comments made from our members that may be useful too – but weren't questions to address as such.

Comment 1

'I registered for the Experian service and was reassured to be contacted by them shortly after an identification check was done as part of me using HMRCs online services.'

Comment 2

'I suggest if you get any alert from Experian that you don't recognise go to the www.actionfraud.police.uk web site and report it - you will get a reference number which should give some protection if, for example, someone e subsequently takes out insurance in your name.'

Comment 3

'Experian didn't ask for bank details, only which banks I am with.'

Comment 4

'Just a comment that I've found Experian easy to use.'

Comment 5

'From my experience Experian don't require you to supply bank or credit card details – they offer it as an option as it gives them more parameters to monitor on the web.'

We'd urge you to set up your Experian service and contact them if you have any questions. If you have other questions that you want to ask Capita, please do be patient with the team. The incident has had an impact on their 'business as usual' processing, and they're recovering from lost time as a result of the cyber incident at an already busy time.