ScottishPower Pensions

These Q&As were last updated on 26 March 2024.

Capita cyber incident

Questions and Answers

Question 1

When did the cyber incident occur?

The cyber incident occurred at Capita plc, was detected on 31 March 2023 and confirmed by Capita by press release on 3 April 2023. Capita took immediate steps to isolate and contain the issue, which 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 a number of pension schemes. Since then, it has undertaken a complex forensic investigation with support from technical experts and specialist advisers.

Question 2

What was the impact of the cyber incident?

Capita confirmed that personal data in relation to a number of pension schemes has been part of the data exfiltrated as a result of the cyber incident.

Question 3

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

Capita confirmed the cyber incident by press release on 3 April 2023 but at this stage we had no information to suggest that our Scheme members were impacted. We were however monitoring the situation and engaging closely with Capita as its internal investigations progressed, to understand if, and to what extent, our members were affected.

Capita wrote to us on 22 May 2023 to inform us that the cyber breach did involve personal data of our Scheme members – at this stage it was mainly pensioner members that appeared to be impacted by the incident.

Question 4

Why has data been retained by Capita following the transition of administration services to Mercer?

Even though the administration of the Schemes moved from Capita to Mercer in January 2022, some Scheme member data is retained by Capita for use in finalising transition activities.

Question 5

What data has been affected?

Initially, Capita informed us that the information affected included: National Insurance number; initials and surname; pension amounts; and some tax information. At this stage, we were advised that it was mainly pensioner members who were impacted. A communication was issued to this group (as confirmed by Capita at that time) and should have been received by 30 June 2023.

However, Capita subsequently wrote to us on 19 July 2023 to confirm that a larger proportion of the membership and additional data fields were affected. The data fields impacted are: name, gender, address, National Insurance number, date of birth, tax information, pension details and in some instances their bank details. These may not be relevant to all members.

Question 6

Where was the personal data when it was accessed?

We understand that the personal data was stored on Capita's file servers.

Capita confirmed that there was no access to their Hartlink member portal.

Question 7

When did you find out that more data was affected?

Capita wrote to us on 22 May 2023 to confirm that Scheme members data had been affected. Capita wrote to us again on 12 June 2023 to advise that further data categories had been impacted but did not provide us with member level information at this time. On 19 July 2023, Capita wrote to us to confirm that, as a result of concluding their internal investigation, additional data for Scheme members had been affected and a larger portion of Scheme members are impacted than they previously advised. They confirmed at this point that the Members impacted include pensioner members, active members (i.e. those still building up benefits in the Schemes) and deferred members (generally ex-employees who have yet to access their benefits). However, some former members of the Schemes have also been affected, e.g. those who have transferred their benefits out of the Schemes into another arrangement.

The Trustee Boards worked with Capita to review and verify the data to allow the Trustee Boards to contact those new individuals who are now affected. We issued a communication to current members of the Schemes on 31 August 2023. This was either by email or letter in accordance with members' preferred communication method. As noted above, some former members of the Schemes who no longer have a benefit in the Schemes were also affected by the incident. The Trustee Boards are considering the approach to contacting former members, who no longer have a benefit in the Schemes, due to concerns about the reliability of historic contact details.

Question 8

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

Capita has publicly stated that it "has taken extensive steps to recover and secure the customer, supplier and colleague data contained within the impacted server estate, and to remediate any issues arising from the incident." You can read the full statement here:

https://www.capita.com/news/update-actions-taken- resolve-cyber-incident.

Capita have stated that there is no evidence that any data has been compromised or is available for sale online as a result of this incident.

Question 9

What advice can you give to affected members to protect themselves?

Capita are offering affected members the option to sign up to a free identity monitoring service with Experian. Each affected member has or will receive a unique activation code to access the service.

We would always encourage members to only ever give out personal information if they are absolutely sure they know who they are communicating with.

- 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.
- We send emails under our communications and administration services provider, Mercer, usually ending **@Mercer.com**.
- If you contact us, we might require you to undertake additional verification requests. We'll never ask for your bank details.
- Don't click on embedded attachments or links within emails unless you know the email has been sent from a reliable source. Viruses can be introduced into computers via emails that contain harmful attachments or links.
- Make passwords long and strong combining at least 8 capital and lowercase letters with numbers and symbols.
- Keep separate passwords for every online account. Search for 'Password Keepers' online to help you manage your passwords.

Whether you've been impacted by this incident or not, in a data-driven world, we recommend that members take steps to protect their personal data and avoid scams.

Members should be alert to suspicious messages and be vigilant in checking their online accounts for any unauthorised activity.

The National Cyber Security Centre and the Information Commissioner's Office (ICO) both provide guidance that may also be useful.
https://www.ncsc.gov.uk/guidance/data-breaches
https://ico.org.uk/for-the-public/

Question 10

How are you protecting the members affected?

We are proactively engaging with Capita in respect of their ongoing investigations and continue to engage with them about the ongoing support they will be providing to those affected.

We are writing to each of the members affected as soon as possible to make them aware and to provide details of the support available to them, advice on next steps and further contact details. Those impacted will be contacted as soon as practically possible after receiving the necessary information from Capita.

Question 11

Is my Mercer OneView account safe?

Yes. This incident does not involve the current Scheme Administrator, Mercer in any way. This includes the online member portal, OneView which is a Mercer owned and operated system.

Question 12

Is my pension safe?

We'd like to reassure all members that your pensions remain secure. No funds from the Schemes were involved and the Schemes' assets are held completely separate from Capita.

Question 13

What safeguards have the Trustees put in place to ensure this doesn't happen under Mercer's watch?

Mercer have confirmed to the Trustees and the Pensions Regulator that they have implemented cyber-attack prevention measures as expected by the Pensions Regulator, to protect your data.

For any member who calls Mercer or wants to make a benefit claim, additional security checks have been added to Mercer's processes to ensure that they verify the person making the claim as legitimate. We would therefore ask for your patience in this process as there may be additional security questions which are designed to protect you and your benefits.

Question 14

What if I wish to submit a query or complain about Capita's cyber incident?

The Trustee Boards appreciate you may have questions regarding the incident. Please be assured that we are working hard to provide as much information as possible regarding the incident and continue to work with Capita to understand the full nature of the incident.

We are working with Capita to understand common questions that are being asked – we will be updating the FAQs regularly to answer these questions for the benefit of all Scheme members, and as more information becomes available. You can find the latest version of the FAQs here for Scottish Power Pension Scheme members and here for Manweb Group of the Electricity Supply Pension Scheme members.

Any queries in relation to the cyber incident or Experian service being offered should be directed as follows:

- Queries in relation to the cyber incident should be directed to Capita's FAQ Contact centre on 0800 229 4005. They are open Monday to Friday 8.30am to 5.30pm and Saturday 9am to 2pm (UK time).
- Queries in relation to the Experian Identity Plus service (for UK based individuals) should be directed to the Experian helpline on 020 8090 3696. They are open Monday to Friday, 8am to 6pm.
- Queries in relation to the Experian Identity Works service (for those based overseas) should be directed to the Experian mailbox: **globalidworks@experian.com**

Any complaints about Capita's cyber incident should be emailed to: **cyber_exitedschemes@capita.com**

Capita are processing and responding to all complaints related to their cyber incident. Please note any complaints in relation to the Capita cyber incident addressed to the ScottishPower Pensions Team, the current administrator Mercer or individual trustees will be sent to Capita in the first instance.

Any general queries or complaints (not related to the Capita cyber incident) should be directed to the current scheme administrators, Mercer Ltd:

By completing an online form via Contact.Mercer.Admin – **https://contact.mercer.com/green**

By phone: 0330 808 1523 for Scottish Power Pension Scheme members and 0330 808 1525 for Manweb Group of Electricity Supply Pension Scheme members.

Question 15

How can members access the Experian service if they are not online?

Capita have confirmed that the service provided by Experian can only be provided online. This is the case for all such services offered in the market.

Question 16

Are you carrying out your own checks?

The Trustee Boards have reviewed their own systems and controls to ensure they remain robust, taking independent professional advice as required. They have also been keeping the Company informed and working with the Company as appropriate.

Question 17

I have received an Experian alert. Does that mean someone is using the personal data accessed during the Capita cyber breach?

The Experian identity monitoring service works by scanning certain internet sites and locations for selected personal and financial details, and alerting you by email or text message if anything looks wrong or fraudulent.

It will track all relevant information on those sites which may be from a variety of sources (including other unrelated cyber incidents), not just any personal information that may have been affected by the Capita cyber incident.

Capita, through an independent specialist organisation, continues to monitor the dark web and to date has not identified any instances of the relevant Capita data being used or purchased by any cyberthreat actors. However, individuals should continue to be vigilant.

Question 18

What are you doing about former members of the Schemes?

Some former members of the Schemes have been affected, e.g. those who have transferred their benefits out of the Schemes into another arrangement. Both Trustee Boards have sought to verify the address details previously held on record for these individuals. Where the address was found to continue to be accurate ,the individuals have been notified of the incident and provided access to the Experian identity monitoring service.

Question 19

Why does the scheme continue to hold my information after I have ceased to be a member?

Like most pension schemes, the Trustee's, via the scheme administrators, hold records for members and ex-members for a variety of reasons. These include dealing with any queries that may arise in relation to your membership of the scheme.

Where members' benefits have been transferred out, it is common for the Trustee to receive queries, sometimes many years later, in relation to members' past benefit entitlements or the circumstances in which transfers were made.

Legal and regulatory developments can also require the Trustee's to look back at the benefits and records of members who have left the Scheme.

Retaining member records enables the Trustee to respond to these queries or developments and ensure it fulfils its legal duty to administer the Scheme correctly and protect the interests of all members, past and present.

Question 20

Why aren't the Trustee Boards or Company doing more?

Please be assured that both the Trustee Boards and Company have taken this incident very seriously. The Trustee Boards have been working with their legal advisers and data technical specialists to make sure that they are undertaking all appropriate steps in relation to the incident.

The Trustee Boards will continue to update these FAQs when relevant information is released, including the findings of the ICO's report when it is issued.

Question 21

The cyber incident was detected in March 2023, why has it taken so long for information to reach me?

The Trustee Boards were able to communicate with most impacted individuals during 2023. For others however additional steps had to be taken to verify address information. The Trustee Boards also published a statement and FAQ on the Oneview portal at the time of the incident and has updated these documents to reflect relevant developments.

Question 22

Have you informed the Information Commissioner's Office (ICO)?

We have reported the issue to the ICO and following recent engagement with the ICO, we do not anticipate regulatory action being taken against either Scheme at this stage.

The ICO is currently carrying out a detailed investigation into Capita's role in the cyber incident and its findings will be publicly available in due course. Please note this may take some time to be published given the scale and complexity of the incident.