This statement was last updated on 1 September 2023

A message from the Trustee of the ScottishPower Pension Scheme and the Manweb Group of the Electricity Supply Pension Scheme (the Schemes) – Important information about Capita's cyber incident

Capita, who previously provided administration services to the Schemes, experienced a cyber incident earlier this year.

ScottishPower
Pensions

As you will be aware, the administration of the Schemes moved from Capita to Mercer in January 2022. Some Scheme data is however retained by Capita for use in finalising transition activities.

The cyber incident was detected by Capita on 31 March 2023 and confirmed by them by press release on 3 April 2023. As Capita's investigations have progressed the Trustee Boards have been in regular contact with Capita to understand if Scheme members were impacted by the cyber incident and, if so, to what extent.

Through this engagement, Capita reassured the Trustee Boards that they had taken steps to isolate and contain the issue. Through their investigations, Capita have identified evidence that certain data has been compromised. Their forensic investigations are ongoing.

Timeline

Unfortunately, we were informed on **22 May 2023** that some personal data which Capita holds in relation to our Scheme members was part of the data impacted by the cyber incident. The impacted population identified in May included a large number of our retired membership, i.e. those receiving a pension from the Schemes.

Communications to these members were issued and should have been received by 30 June 2023 via the member's preferred communication method (email or post).

Capita subsequently notified us on **12 June 2023** that additional personal data had been impacted for some of these members. They also indicated that more Scheme members were impacted than previously advised. We have been working with Capita to understand the extent of the additional information, member categories involved and the individual members who are impacted.

Following a further communication from Capita on **19 July 2023** we now know that the impacted population extends to the majority of current members of the Schemes. This includes the majority of active members (i.e. those still building up benefits in the Schemes), deferred members (generally ex-employees who have yet to access their benefits) and retired members (pensioner members). 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.

We issued a communication to the current members of the Schemes on 31 August 2023. 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.

Next Steps

As you can see from the above timeline, the developing impact of this incident has been very complex, and it has taken some time for Capita to fully and accurately identify which of our members have been impacted and to what extent.

As mentioned above, Capita continue to carry out assurance and validation of their investigations. The Trustee Boards will continue to engage with Capita as appropriate and will continue to keep members updated via the portal and directly where appropriate to do so.

We regret that members' data has been accessed in this way. We would like to emphasise that this incident does not involve the current Administrator of the Schemes, Mercer, in any way. This includes the online member portal, Oneview, which is a Mercer owned and operated system.

Both the Information Commissioner's Office (ICO) and the Pensions Regulator are aware of the Capita cyber incident, and we will continue to update them on developments. In the meantime, there are actions you can take to keep your personal data safe. We would 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.

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/