Capita cyber security incident

As you may be aware from recent press reports, Capita recently reported a cyber incident involving hackers targeting some of its computer servers – potentially affecting several of the cross-sector businesses it serves.

Capita provides administration services to the Rhodia Pension Fund (the "**Fund**") and as part of this service they process personal data of Fund members. The Trustee has been communicating with Capita since it became aware of the cyber incident in order to establish whether the personal data of Fund members may be affected by the breach. This incident has been very complex and it has taken some time for Capita to confirm the impact of the incident on the pension schemes that it acts for.

The Trustee was informed on Thursday 8 June 2023 that, regrettably, details of Fund members were held on the Capita servers accessed by the hackers. Capita has confirmed that the personal data accessed includes:

- Members' names; addresses; dates of birth; National Insurance numbers; pensions in payment; tax codes; tax paid and any other deductions where applicable; Fund member identification numbers; and bank details.

Capita has confirmed that the data breach extends to roughly 3,300 members of the Fund, most of which are members with pensions in payment. The Trustee is writing to each affected member individually. You will not receive a letter if you are not in the list of affected members.

Possible consequences of the data breach

There are a number of possible consequences that may arise for affected members as a result of the data breach. You may be at an increased risk of identity fraud, and/or a target for pension scams or malicious emails. We have set out below some steps you can take to protect yourself from the risk of pension scams.

Steps that you can take

We recommend that you are extra vigilant in respect of companies that contact you out of the blue, such as cold-calls, emails or texts, no matter how trustworthy or official they seem. Remember, don't be rushed or pressured into making any decisions about your pension. Pension cold calling is illegal, and you should be very wary if you are approached in this way.

Cyber criminals commonly use a scam technique called "phishing", which is mostly email-based but can also be via telephone calls, to lure victims under false pretences to websites which look legitimate to get them to provide information including bank account and credit card details. These emails/phone calls appear to be from recognisable sources such as banks but actually link to fraudulent websites. 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.
- If you are concerned someone might be impersonating the Trustee or Capita, please let us know by emailing Rhodia@capita.co.uk

To help reduce the risk of identity fraud:

- Protect your email with a strong password (tip: use 3 random words to create a single password that's difficult to crack).
- Do not share your password with anyone.
- Install the latest security updates to your browser software and personal computing devices.
- If in doubt, do not open emails from senders you do not recognise.
- Check links look correct before you click on them.
- Be suspicious of anyone who asks for your bank account or credit card details.
- If the email contains spelling mistakes, this can be a sign that this is a phishing scam. Do not open the email or attachments.
- If you think you have been a victim of fraud you should report it to Action Fraud, the UK's national fraud and internet crime reporting centre, on 0300 123 2040.

We recommend that you seek authorised financial advice before making any pension decisions. You could also contact MoneyHelper, which provides free, independent and impartial information and guidance. MoneyHelper can be contacted on 0800 011 3797 or at https://www.moneyhelper.org.uk/en/contact-us/pensions-guidance.

You can also access the Financial Conduct Authority's (FCA) ScamSmart resources and check their register of regulated advisers to make sure anyone offering you advice is authorised by visiting its website - https://www.fca.org.uk/scamsmart. If they are, check they're allowed to give pension advice, by calling the FCA helpline on 0800 111 6768, where you can also report suspected scammers.

You can also find out more about keeping your pension safe from scammers on The Pensions Regulator's dedicated page: https://www.thepensionsregulator.gov.uk/en/pension-scams.

What is the Fund doing to resolve this matter?

We appreciate that this matter will be of great concern to a lot of Fund members, and we are very sorry that this has happened. The Trustee is proactively liaising with Capita to obtain further details about the breach and the actions Capita are taking and will provide affected members with all the support we can.

Capita has confirmed to the Trustee that:

- It has appointed a third-party specialist adviser that continues to monitor the internet to confirm that data compromised as a result of this incident is not circulating more widely.
- That third party has reported to Capita that they can find no evidence that data resulting from this incident is further circulating on the internet (including the dark web) or otherwise.
- It has taken extensive steps to recover and secure the data contained within the servers impacted by the incident.
- It has made its own report to the Information Commissioner's Office ("**ICO**") and is working closely with other regulators and authorities, namely the Financial Conduct Authority, The Pensions Regulator, and the National Cyber Security Centre

In addition to providing this notice (and separate from the letter which you will receive if Capita has confirmed that you are one of the members affected), the Trustee will be sending a further letter to members in due course to provide an update on the position and, for each affected member, confirm the categories of personal data that have been affected by this incident.

The Trustee reported this breach to the ICO on Friday 9 June 2023 (the day after the Trustee became aware that Fund members were affected). The Trustee has also independently informed The Pensions Regulator of the breach.

Further information

A copy of the Fund's privacy notice setting out how we process your personal data is available on the Fund website. Members can also contact the Fund using the following details if they have any queries in relation to the Capita incident or the way in which their data is processed more generally: telephone 0344 3912 403 or email Rhodia@capita.co.uk

Capita has also released several statements in relation to the incident, which can be accessed here: www.capita.com/news

The National Cyber Security Centre (https://www.ncsc.gov.uk/guidance/data-breaches#section_3) and the Information Commissioner's Office (ICO) (https://ico.org.uk/for-the-public/) both provide guidance that may also be useful in relation to this matter. You can contact the ICO directly by telephone (0303 123 1113). Alternative ways to contact the ICO are available at: https://ico.org.uk/global/privacy-notice/how-you-can-contact-us/

The Trustee offers its sincere apologies for this incident and will continue to closely monitor the situation and work with Capita to ensure that its security processes are improved and steps are taken to prevent an incident of this nature happening again.