

## **CAPITA CYBER INCIDENT – MEMBER FAQs**

### **Where did the cyber incident occur?**

The cyber incident occurred at Capita plc, a provider of outsourced services to thousands of clients. The incident impacted a small number of its computer servers. This included some used by Capita Pension Solutions Limited (“Capita”), which is a business that, until March 2023, provided pension administration services to members of the ConocoPhillips Pension Plan (“the Plan”), along with many other major pension schemes.

### **When did it happen?**

Capita announced on 3 April via its public website that it had suffered a cybersecurity incident on or around 31 March 2023, leading to the disruption of certain servers in its systems.

Following receipt by ConocoPhillips Pension Plan Trustees Limited (“the Trustee”) of Capita’s notification, the Trustee took immediate steps to contact Capita to find out more information about the cybersecurity incident and in particular to confirm whether Plan data had been affected, or not. At that time, Capita was unable to confirm whether Plan members’ personal data was affected. We understand from Capita that Capita isolated and contained the issue and has undertaken a forensic investigation with support from technical experts and specialist advisers. This has involved reviewing files across Capita’s business.

### **When were you first made aware that member data had been affected? [\[Updated\]](#)**

We have been working closely with Capita since it first announced the cyber incident and have sought regular updates on the progress of its investigation.

We were formally informed of a personal data breach affecting Pensioner members of the Plan only on 18 May 2023 and shortly after we received information about the data which was impacted.

On 13 June 2023, we were formally informed by Capita of additional data impacts to our Pensioner members and in subsequent discussions with Capita that Active and Deferred members were also affected. The data at risk was confirmed by Capita on 21 June 2023 and varies by affected member group.

### **Does this impact all members? [\[Updated\]](#)**

Based on the latest information available from Capita, all members were affected. However, the data at risk varies by member group as described in the FAQ ***“What Data is at Risk?”***

**Have you contacted all affected members? [Updated]**

Yes, we have written to all Plan members.

Our letters highlight the affected data and potential risks, provide details of how to access “*Experian Identity Plus*” for UK-based members and “*Experian IdentityWorks<sup>SM</sup>*” for overseas members, a credit and web monitoring service provided free of charge by Experian, one of the UK’s leading Credit Reference agencies, and the steps members can take to protect their personal data.

A link to a number of useful websites where members can obtain additional general information and helpful guidance is also provided.

**Has this affected pension payments made to members?**

No, as notified in a communication from the Trustee to members in February, Capita was replaced as the Plan’s service provider for administration services effective 7 March 2023. All pension payments have since and will continue to be paid by the new provider, Barnett Waddingham.

**Is my pension safe?**

We would like to reassure all members that your pension remains secure. The Trustee has robust security protocols governing the use of personal data and payment of benefits in place.

The Trustee is familiar with The Pensions Regulator's guidance on cybersecurity principles for pension schemes and has received training on approaches to mitigate cyber risks and protect member data should either a cyber or data breach occur. The Trustee seeks assurances from its advisers and service providers regarding the safety procedures they have in place.

As part of the Plan’s due diligence, Barnett Waddingham, the new Plan Administrator that recently replaced Capita, will be monitoring Plan activity for increased or unusual transfer requests and will be reporting to the Trustee on the same.

**What data is at risk? [Updated]**

For the majority of members (Active, Deferred and Pensioner), the information potentially accessed includes:

- Title
- Forename
- Surname
- Gender
- Your unique Plan ID
- National Insurance number
- Pensionable salary details
- Address
- Date of Birth
- Telephone number (where provided to Capita)
- ConocoPhillips employment dates

For **Deferred members**, the following additional data is at risk:

- Rate of accrued pension

For **Pensioner** members, the following additional data is at risk:

- Bank details
- Rate of pension in payment
- Retirement date
- Recent tax information

While Capita's internal investigation is complete, the investigation by Capita's third-party specialist adviser is ongoing and is not yet complete. Should we learn of any additional member data that may have been affected, we will notify those members directly.

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

Capita has advised us that it cannot be certain that the personal data has been accessed. However, we believe it is appropriate to warn members about the potential risk and the possibility that personal data could be used for fraud, identity theft, or to send malicious email. 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>

#### **Is the Trustee required to notify any regulators about the incident?**

We are required to inform the Information Commissioner's Office (ICO) and The Pensions Regulator.

We have reported the impact on member data to both the ICO and The Pensions Regulator and will work with them on any investigation they choose to conduct and any recommendations they may make. Moreover, we are currently evaluating whether other regulatory notifications are required pending further information from Capita.

#### **How are you protecting the members affected? [Updated]**

We are proactively engaging with Capita regarding their ongoing third-party investigations and are considering the next steps available to us. Affected members will be given the opportunity to opt-in free of charge to a credit and web monitoring service provided by Experian for a period of 12 months.

Information on this service has already been provided to the initial group of members identified as being affected (Pensioners) and based on new information received from Capita that Active or Deferred Members are also impacted, these members are now also eligible and will receive further information week commencing **26 June 2023**.

### **If I am an Active or Former Member of the Plan, will I be able to access the identity protection service being offered by Capita? [Updated]**

Yes, Capita is offering access to the identity protection service to members of the Plan whose data has been identified to be at risk. Details of how to activate your membership will be provided week commencing **26 June 2023**.

### **Where can I get more specific information related to the incident?**

Please visit Capita's website at <https://www.capita.com/news> for the latest updates relating to this incident.

### **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 would encourage members to only ever give out personal information if they are absolutely sure they know who they are communicating with. Members are advised to remain vigilant and report any suspicious activity.

- If you receive a suspicious email, you should forward it to **report@phishing.gov.uk**.
- For suspicious text messages and telephone calls, forward the information to **7726** (free of charge)
- For suspicious items received via post, contact the business concerned.

The following websites provide guidance that may be useful; we have also provided contact details where a telephone service is available:

- The National Cyber Security Centre
  - <https://www.ncsc.gov.uk/guidance/data-breaches>
  - Enquiries Team **0300 020 0964**
- The Information Commissioner's Office (ICO)
  - <https://ico.org.uk/for-the-public>,
  - ICO helpline **0303 123 1113**
- The Pensions Regulator
  - <https://www.thepensionsregulator.gov.uk/en/pension-scams>

**What further steps are you taking to protect my data?**

In our discussions with Capita, we have sought information about what it has done to improve the security of personal data and avoid a future incident. We will continue to work with Capita to obtain a full report about the incident, how it was managed and what steps Capita will take to further mitigate risk to members.

The Trustee is familiar with The Pensions Regulator's guidance on cyber security principles for pension schemes and has received training on approaches to mitigation of cyber risks and protection of member data should either a cyber or data breach occur. The Trustee seeks assurances from its advisers and service providers regarding the safety procedures they have in place.

**You advised that some Plan data was impacted by Capita's incident; can you please confirm if the data at risk includes banking information? [\[Updated\]](#)**

Capita has recently informed us that their internal investigation, which is now complete, identified some further Pensioner data, including banking information, that was part of the data exfiltrated.

The complete summary of personal data confirmed by Capita as being at risk is detailed above under the FAQ "***What data is at risk?***"

**I am a pensioner member, when should I expect to receive details of the Experian credit checking and web monitoring service that is being provided by Capita? [\[Updated\]](#)**

A letter outlining the features of the "***Experian Identity Plus***" and "***Experian IdentityWorks<sup>SM</sup>***" for overseas members, and the steps to be taken to activate your membership, was issued to all Pensioner members' home addresses week commencing 12 June. A further letter containing this same information will be issued week commencing **26 June 2023**.

**I have recently received a communication asking me to register for Member Self Service with Barnett Waddingham – is this a genuine request?**

Yes, Deferred and Pensioner Plan members should have received a letter/e-mail, and Active members an e-mail, from Barnett Waddingham in May. The communication will have displayed both the ConocoPhillips and Barnett Waddingham logos at the head of the letter/email and will have displayed a BWebstream registration key specific to you at the top right-hand side of the page. This request is legitimate.

**What should I do now that Capita has advised that Pensioner member's banking information is at risk? [\[New\]](#)**

If you are a Pensioner member, you should notify your bank of the incident and request multi-factor authentication be added to your financial account(s), where possible; you may also wish to consider asking for your credit to be frozen to prevent identity theft.

**Are you able to share any guidance for members on ‘general’ good practices for protecting personal information? [New]**

ConocoPhillips seeks to continually build an environment that protects employees, benefit program participants, assets, data, resources and products. As we build that cyber security culture, we encourage all stakeholders to extend those practices into their everyday lives. Staying vigilant builds a stronger defense for us all. Details of best practices to protect your personal information may be found at: <https://static.conocophillips.com/files/resources/best-practices-to-protect-your-personal-informatio.pdf>.

**Is the Experian offer legitimate? [New]**

The Experian offer outlined in the Trustee communications is legitimate; membership which may be activated using the code provided in the Chairman’s letter, is being provided to members for a period of 12 months free of charge.

**If you have questions that are not covered here, please contact HR Connections +44 (0)808 234 1519 between 14:00 and 23:00 BST, Monday to Friday.**

Date published: **26 June 2023**