Commonwealth War Graves Commission

Superannuation Scheme

20 May 2024

Cyber Incident – Personal Data

Capita, the pensions administrators for the Scheme, experienced a 'cyber incident' in March 2023 which arose following initial unauthorised access to data held by Capita.

As a result of Capita's investigations, they informed the Trustees on 19 May 2023 that personal data which Capita process on our behalf has been part of the data extracted as a result of the cyber incident. Unfortunately, the data includes personal data relating to members of the Scheme. Capita appointed third-party eDiscovery experts to forensically review the data exfiltrated from the affected servers. They have recently completed that independent review and have informed Capita that, apart from members who were notified in 2023 that their data has been extracted, further members of the Scheme have had their data extracted. In addition, for some existing affected members, the review has identified that additional types of personal data were extracted above the personal data which was originally identified.

Details of all of the categories of extracted personal data are set out below, and the additional and existing members who are affected by the 2024 update have been notified. Capita have informed us that this data breach related to the following areas, as updated:

- Name
- Unique member identification
- National Insurance Number
- Pension in Payment
- Tax Code
- Tax Paid and any other deductions where applicable
- Date of Birth
- Date of Retirement
- Date of Cessation of Pension
- Bank Details
- Address

This means that for some members, some or all of this data may have been extracted by the hackers. We understand from Capita that the independent review has identified 10 additional members who were affected and that some additional categories of data have been identified for approximately 370 of the members previously contacted. To be clear, this does not necessarily mean that the data has been identified as exfiltrated, but we believe it is appropriate to act as if there is a likelihood this is the case. We want to be transparent with you about the potential risks so that you can determine if you need to take precautions.

We have been working with Capita since May 2023 to identify the members affected and contact them so that they can take steps to protect themselves and minimise the potential impact of this incident. We will continue to do so in respect of members affected as a result of the updated review. Letters have been sent to members affected by this latest update.

Capita has informed the Information Commissioner's Office ("**ICO**") about the cyber incident and has been in regular contact with all relevant authorities. We have also made a separate report to the ICO, and have also informed the Commonwealth War Graves Commission ("**Commission**") and the Pensions Regulator.

As a result of the data which has been taken, we consider this incident presents a risk that member information could be used for suspicious or potentially criminal activity. There is a possibility that if the information is accessed it could be used for fraud, identity theft or to send malicious emails, although Capita has no evidence that information resulting from this incident is available for sale on the dark web or otherwise. That is because Capita has 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.

We realise that this will be a concern to you. We apologise for this, and we want to reassure you that we continue to take steps alongside Capita to try and minimise the effect of this incident and reduce the likelihood of harm. As part of this, affected members were given access to a leading identity protection service for 12 months free of charge if they so desired, and newly affected members will also be offered this opportunity. We have contacted affected members to explain to them how that will work and what they need to do to gain access to the service.

We would also encourage you to continue to protect yourself as much as possible by looking at the guidance provided on the following websites, and learning the signs of possible identity fraud, phishing and other cyber-crimes:

The National Cyber Security Centre - https://www.ncsc.gov.uk/

The Information Commissioner's Office - https://ico.org.uk/for-the-public/

For more information on pension scams, and how to spot a scam, visit https://www.fca.org.uk/consumers/protect-yourself-scams .

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.

In addition:

- 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.
- If you do receive any suspicious messages or calls, please do not hand over any information such as your bank account details.
- If you receive a suspicious email, you should forward it to report@phishing.gov.uk .
- For text messages and telephone calls, hang up and 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 the Trustees or the Commission in relation to your pension arrangements, please act with caution and ask the person to provide full identification and information before providing them with any information or taking any further action as a result of that contact.

Affected members have received letters in the past, and, in 2024, newly affected members or members where additional extracted information has been identified should have received letters, so that we can support them and minimise the risks associated with this incident. If you have not received a letter, we understand from Capita that your data has not been exfiltrated. We still believe however that, for safety, you should still act as if there is a likelihood that you have been affected.

Once again, we are sorry for the distress and inconvenience this incident has caused or will cause you, and we want to reassure you that once we became aware of it, we have acted swiftly to try and reduce the likelihood of negative effects.

The Trustees of the Commonwealth War Graves Commission Superannuation Scheme