Capita Cyber Incident Affecting G4S Pension Scheme Pensioners

(Announcement date: June 2023)

You may have seen in the news that Capita, who provide pension administration services to the G4S Pension Scheme, has recently experienced a cyber incident. Most members of the G4S Pension Scheme are former employees. The pension plan that G4S offers to the vast majority of current employees was not affected.

Files containing pensioners' personal data, which could include name, National Insurance Number and date of birth, have been identified on an affected server from which data was exfiltrated as a result of the cyber incident.

Capita has written to the affected members on behalf of the Trustee providing further information and support. Therefore if you are affected then you should have received a letter.

Capita has confirmed to the Trustee that only pensioners are affected. Therefore if you are not yet receiving a pension from the G4S Pension Scheme you have not been affected.

We appreciate that this is worrying news, but we felt it important to make affected members aware of the situation so that they can remain vigilant and check for any suspicious activity on bank or credit card statements.

Capita has been in regular contact with all relevant authorities, including the Information Commissioner's Office, The Pensions Regulator, The Financial Conduct Authority and the National Cyber Security Centre. The Scheme has also been in regular contact with relevant regulators.

We want to assure you that Capita has taken extensive steps to recover and secure the data contained within the servers impacted by the exfiltration and has appointed an independent cyber security expert who continues to monitor the web to confirm that data compromised as a result of this incident is not available.

The trustee would like to apologise for any inconvenience and concern this incident has caused members and will continue to work with Capita to make sure support is available for members who are impacted. We take the responsibility of protecting members' personal data very seriously and we have sought information about what Capita has done to improve the security of personal data and avoid a future incident. We want to reassure you that your pension remains secure.

If you have any questions regarding this cyber incident, please contact the helpline on 0800 2294005, Monday to Friday – 8.30 to 5.30 + Saturday – 9.00 to 2.00.

What can you do?

You can find information on how to spot scams on the Pension Scams page. The link is below. The National Cyber Security Centre website also provides guidance that may be helpful. https://www.ncsc.gov.uk/collection/phishing-scams

We encourage everyone, whether or not they are directly affected by this, to stay alert against any suspicious calls, texts or emails which could be a scam. If you do receive any suspicious messages or calls, please do not hand over any information such as your bank account details. Instead, hang up, or delete any worrying texts or emails. The FCA has some useful information on how to spot the warning signs of financial scams at https://www.fca.org.uk/consumers/protect-yourself-scams.

The National Cyber Security Centre has guidance on data breaches at https://www.ncsc.gov.uk/guidance/data-breaches

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. Accordingly, we have the following guidance to help reduce the risk of falling foul of these phishing attempts:

• 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.

The Information Commissioner’s Office is the UK's independent body set up to uphold information rights. Its website is a good source of more information about how to protect your personal data online when using computers and other devices: https://ico.org.uk/for-the-public/online