SOPRA STERIA RETIREMENT BENEFITS SCHEME ("THE SCHEME")

CAPITA CYBER ATTACK – IMPORTANT IMFORMATION ABOUT YOUR PERSONAL DATA

Capita provides administration and payroll services to the Scheme. Capita has advised the Trustee that some information has unfortunately been put at risk following a cyber incident at Capita that took place in March 2023. In this announcement we explain what has happened, how your information may be affected and what we are doing about it.

Background

You may have seen news that Capita, who is the Scheme administrator, recently experienced a cyber incident involving unauthorised access to its systems.

Since the incident, the Trustee has had an ongoing dialogue with Capita as it has completed detailed investigations of the incident and its systems. In addition, we are working with the Pensions Regulator and the Information Commissioner's Office (ICO) to investigate this occurrence, because we take the protection of your information very seriously.

Capita has now completed its investigations and regrettably informed the Trustee that files containing some personal data for members and ex-members of the Scheme was impacted by this cyber incident.

If your personal data was impacted by this incident, and if the Trustee has up to date contact details for you, the Trustee has written to you (or will be writing to you shortly) providing details of the steps that Capita has taken and providing some guidance for you on how to protect your own data.

There is a possibility that where personal data has been accessed it could be used for fraud, identity theft or to send malicious emails, although Capita has advised that it has no evidence that information resulting from this incident has been misused or that it is available illegally including on any third-party websites.

Capita has assured the Trustee that it has taken extensive steps to recover and secure the data contained within the servers impacted by the data incident, and has advised that it 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.

We are sorry for any distress that this news may cause you. The protection of your personal information is a top priority for us and we want to assure you that we are doing everything we can to minimise any risk. We wanted to take this chance to reassure you that we are working closely with Capita to minimise the impact on our members, and if there is anything more you need to do, we will write to you and let you know (if we have your address) and we will post any further updates on this website. If you are not sure that we hold a correct address for you, or if you are not sure what address is held for you, you should contact Capita with your current home address, email address and phone number by emailing steria@capita.co.uk. In the meantime, please read the information below to ensure that you take all necessary actions to ensure your data is protected.

What steps can you take?

We encourage you 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.
- Check your bank statements regularly for any unusual payments that you do not recognise, or if payments you are expecting are not received.
- If you use online services or telephone banking, always use strong passwords, and change them regularly. Try to keep them at least eight characters long and use a mix of numbers, upper case, lower case, and symbols. Avoid using words which may relate back to you (for example, family member names or dates of birth).
- 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.

We would like to apologise for any inconvenience and concern this incident has caused you and would like to reassure you that we will continue to do everything we can to work with Capita to make sure support is available for members who are impacted.

If you have any questions regarding this cyber incident, please email the Trustee at pensions@soprasteria.com

Frank Oldham
Chair of the Trustee of the Sopra Steria (Retirement Benefits Scheme) Trustees Limited
June 2023