SOPRA STERIA RETIREMENT BENEFITS SCHEME AND
STERIA ELECTRICITY SUPPLY PENSION SCHEME ("THE SCHEMES")

FREQUENTLY ASKED QUESTIONS ("FAQ") DOCUMENT RELATING TO THE CAPITA CYBER INCIDENT

VERSION 2 – DECEMBER 2023

This is the second version of the FAQ document issued by the Trustees in relation to the Capita cyber-incident. New questions have been added at 6, 7, 34, and 35 (altering the following numbered points), and the response to question 26 (previously 24) has been updated to reflect further action taken by the Trustees on your behalf.

The Capita Cyber Incident. What is it? When did it happen? How does it affect me?

1. What is the role of the Trustees in relation to the Schemes?

Sopra Steria (Retirement Benefits Scheme) Trustees Limited is the Trustee of the Sopra Steria Retirement Benefits Scheme and Steria Electricity Supply Pension Trustees Limited is the Trustee of the Steria Electricity Supply Pension Scheme (referred to collectively as "the Trustees"). The Trustees are responsible for managing the Schemes' assets in the interests of the Schemes' members and other beneficiaries, in accordance with the Schemes' Rules and governing legislation.

The Trustees are supported by Sopra Steria Limited, the sponsoring employer who is committed to supporting the Schemes ("the Company"). Whilst these organisations interact, they are themselves independent entities.

2. Who is Capita and what services does Capita provide to the Schemes?

Capita provides administration, pensioner payroll, treasury, and accounting services to the Schemes.

To provide these services, Capita holds personal data for Scheme members (and ex-Scheme members) on its computer servers.

3. What is the Capita cyber-incident?

Capita experienced a cyber-incident in March 2023 involving hackers targeting some of its computer servers, potentially impacting many of its clients, including the Schemes.

Capita regrettably confirmed that the Schemes' member data (including some data for ex-members of the Sopra Steria Retirement Benefits Scheme) was held on the servers that were attacked and, as such, all such members are potentially impacted by this cyber-attack.

4. When was this data breach detected and how was this discovered?

Capita advised that it first became aware of the cyber-attack through its monitoring processes on 31 March 2023. Capita immediately investigated this incident and found that a third party, unauthorised by Capita, had gained access to Capita's IT systems on 22 March 2023. Capita interrupted and restricted the cyber-attack on 31 March 2023.

Capita then announced to all of its clients that it had been the victim of this cyber-incident in early April 2023.

5. Why did it take so long for the Trustees to become aware of this, and why did it then take the Trustees so long to inform the members?

As soon as the Trustees became aware of this cyber-incident, they set up an Emergency Committee comprising the Chair of the Trustees, two other Trustees, the Pensions Manager, the Schemes' legal advisers, and a data breach specialist from Sopra Steria. The Emergency Committee asked Capita (on a daily basis) to confirm whether the Schemes' members had been impacted by this incident.

Capita advised the Trustees that its initial forensic investigations were underway in early April 2023. On 18 May 2023, Capita further advised the Trustees that some of the Schemes' members may have been impacted by the cyber-incident. At that time and based on Capita's investigations to that date, Capita advised that it was pensioner members alone that had been impacted by this incident, although it acknowledged that its investigations were still continuing.

The Trustees requested that Capita issue letters on its behalf to pensioners to inform them that some of their personal data may have been impacted, and to other members of the Schemes advising that this cyber-incident had occurred. The letter also confirmed that Capita's investigations were ongoing. These letters were passed to Capita to issue on 24 May 2023 and were issued the following day.

Capita then advised the Trustees on 6 June 2023 that, following further investigations, additional personal data for pensioner members (including bank details) may have been impacted. The Trustees drafted a further letter to the affected members, which Capita issued on 8 June 2023.

Capita then provided the Trustees with a further update on 11 June 2023, advising that it had finalised its investigations and, in doing so, had identified that other members of the Schemes had been impacted by this incident. The Trustees sought clarity on this and asked Capita to confirm which members had been impacted and what personal data was potentially at risk. Once this clarity had been obtained on 16 June 2023, the Trustees and its advisers drafted further letters to the affected pensioner members and passed these to Capita to issue on 23 June 2023. The Trustees then drafted letters to the remaining members and passed these to Capita to issue on 5 July 2023.

Capita issued all of these letters to the affected current members of the Schemes on 17 July 2023, after going through its own data merge process. The Trustee was disappointed that these letters were not issued sooner by Capita.

In July 2023, Capita also confirmed to the Trustees that ex-members of the Sopra Steria Retirement Benefits Scheme (or ex-members of the earlier pension schemes (see question 34)) had also been impacted by this cyber-incident.

6. Why did it take until October 2023 for ex-members of the Sopra Steria Retirement Benefits Scheme to be made aware of this cyber-incident?

After the Trustees became aware that this cyber-incident had impacted ex-members of this scheme, they immediately drafted a letter to the impacted ex-members. As ex-members are not required to advise Capita when they move house and the Trustees did not wish to send letters to out of date addresses, they first requested that Capita verify the home addresses held by them for all impacted ex-members. There are a large number of ex-members and it took the Capita tracing team some time to verify, or otherwise, the addresses. Once this exercise was completed, the letters were sent on 27 October 2023 to all ex-members for whom Capita was able to verify an address.

7. Why did the Trustees retain my personal data when I left the Schemes many years ago?

Although you may have left the Schemes many years ago, it is necessary for pension schemes to retain personal data for long periods of time, as there are occasions when benefits and records need to be verified many years afterwards, such as to meet legislative requirements and changes in individual circumstances.

8. How many Scheme members were impacted by this cyber-incident?

Based on information provided by Capita, <u>all</u> current members of the Schemes (including pensioners and deferred members) and all ex-members of the Sopra Steria Retirement Benefits Scheme were impacted by this cyber-incident.

All current and ex-members of the Schemes who were impacted by this cyber-incident have been written to by the Trustees of the Schemes, where an up-to-date address is held by Capita.

9. What items of personal data were compromised by this cyber-incident?

Capita has advised that, based on its investigations, the following personal data items were potentially accessed as a result of the cyber-incident:

- Name (title, initials, surname).
- Address and postcode.
- Member unique identification number(s).
- National Insurance Number.
- Date of Birth.
- Date of Retirement.
- Email address (where held by Capita).
- Phone number(s) (where held by Capita).
- Gender.
- Employment details and history (including dates of employment and historic salary details).
- Marital status.
- Maiden name (where applicable).
- Spouse details.
- Bank details, in cases where payments were made from the Schemes to individuals (sort code, account number, and account name).
- Pension details and history.
- Tax codes and tax deducted from pension.

Please note that the data accessed for each member or ex-member of the Schemes was often a subset of the data items listed above, and not all of the above data items were accessed for all members of the Schemes.

The Trustees issued letters to the current and ex-members of the Schemes, confirming the personal data items for each individual member that were potentially impacted by the cyber-attack on Capita.

10. How might my personal data be used by criminals?

Data thieves sometimes use personal information to apply for credit (for example, obtaining credit cards or store cards in your name, or applying for insurance policies).

To try to protect yourself against this, you can sign up to Experian Identity Plus, details of which are in the letters you received from the Trustees. The Experian service has a helpful tool that enables you to "lock/unlock" your credit search facility. This facility is used by companies who carry our credit searches if a credit card application is made in your name. Experian's CreditLock tool allows you to control when you will allow credit searches to be undertaken. Remember that you will need to unlock this if you wish to make a new card application.

Please note that CreditLock will not stop credit limit changes on existing accounts, employment and rental checks, or quotations for credit products. It will not stop new applications for insurance policies, but it may stop applications to pay for insurance policies in instalments (i.e. by direct debit). Further detail on how CreditLock works is available on the Experian website.

You can also carry out a quick, free check on your credit file to make sure nothing unusual has shown up, using sites such as Credit Karma, Clear Score, or the Money Saving Expert Credit Club. You can also use sites such as these to set up alerts that will let you know if anything new appears on your record.

You can find useful resources and tips on protecting yourself and your personal information by referring to the earlier letter from the Trustees.

11. What actions has Capita taken to contain this cyber-attack?

The Emergency Committee continues to engage with Capita in relation to this cyber incident on a weekly basis.

Capita has advised the Trustees that it has taken "extensive steps to recover and secure the data contained within the servers impacted". The Trustees cannot comment on what actions Capita has taken to make such a statement.

Capita has also employed an independent cyber security expert, who continues to monitor the dark web twice daily to confirm that the compromised data from Capita is not circulating more widely. Capita has confirmed that it has found no evidence to date that any such data is available for sale online.

12. What measures are being taken by Capita and by the Trustees to prevent further losses of personal data?

Capita has confirmed that it restored the impacted services and has put more controls in place since this incident occurred.

The Trustees have commissioned a third party cyber expert to review the controls that are now in place within Capita.

The Trustees are regularly liaising with both the Information Commissioners Office ("ICO") and the Pensions Regulator in relation to this cyber-attack. The Trustees informed the ICO of the cyber-attack the day after they were made aware of it (19 May 2023), and Capita has advised that they also reported the attack to the ICO as soon as it became aware of the cyber-attack.

13. What do you mean when you refer to the "dark web"?

The dark web is a hidden collective of internet sites only accessible by a specialized web browser. It is used for keeping internet activity anonymous and private, which can be helpful in both legal and illegal applications. While some use it to conduct legal activities, it has also been known to be utilised for highly illegal activity.

14. Are our pensions safe with Capita?

The cyber-attack against Capita has not impacted the funding of the Schemes, which remain positive, and has not had an adverse effect on the support being provided by the Company, nor on the security of the Schemes' benefits.

Although this cyber-incident has resulted in some delays in some circumstances, the Schemes remain able to pay all benefits as and when they fall due.

15. How can Capita be sure that my data has not been misused or is available illegally?

Capita has employed an independent cyber security expert who continues to monitor the dark web twice daily to confirm that the compromised data from Capita is not circulating more widely. Capita has confirmed that it has found no evidence to date that any such data is being circulated.

Capita has also advised the Trustees that it has taken "extensive steps to recover and secure the data contained within the servers impacted".

16. Capita states that it has employed a third party specialist to monitor the dark web for the Schemes' data. How long will this appointment continue and are the Trustees considering appointing their own third party to monitor the dark web?

Capita has confirmed that the third party specialist that is monitoring the dark web on its behalf will continue to monitor the dark web for the next 12 months, but it is possible that this appointment will be further extended.

To date, the Trustees have not appointed a third party to separately monitor the dark web.

17. What information can be accessed at Capita, using the personal data that was stolen?

Capita has introduced enhanced security questions for anyone who calls in and requests information or tries to make changes to their personal data. For security reasons, the Trustees are unable to state what these controls are.

18. Are any other pensions affected by the Capita cyber incident?

Yes. The majority of Capita's pension clients were impacted by this cyber-attack.

How can I protect my data and what is the Experian offering?

19. What steps should I take to protect my personal data and my identity?

There are a number of simple steps you should take now and, in the future, to keep yourself safe and minimise any risks, some of which are set out below:

- It's good practice to be keep an eye out for anything unusual in your email inbox or arriving by post.
- If you receive a suspicious email, you should forward it to report@phishing.gov.uk.
- If you receive unexpected text messages or telephone calls, do not provide any personal information if this is requested. If someone calls you, please call them back on a number you know is from a true source.
- For any suspicious information received in the post, contact the business concerned directly.
- Check your bank statements regularly for any unusual payments that you do not recognise, or if payments you are expecting are not received.
- Undertake a credit report check for newly opened accounts or credit searches that you do not recognise. Capita is offering a free service with Experian.
- If there are any changes to your National Insurance information, HM Revenue & Customs would contact you directly – but you can also phone them on 0300 200 3500 if you are in any doubt.
- 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 National Cyber Security Centre has lots of useful advice for steps you can take if your data has been accessed or used without your consent at the following website:

  https://www.ncsc.gov.uk/guidance/data-breaches.
- In addition, there is lots of helpful advice and information relating to scams and fraud on the Age UK website:

  https://www.ageuk.org.uk/information-advice/money-legal/scams-fraud/.

20. Do I need to contact my bank(s) to make them aware of this cyber-attack? Should I ask my bank to put a watch on my bank account?

If the letter to you confirmed that your bank details may be impacted by this cyber-attack, it may be advisable to inform your bank of this. You should also check your bank statements regularly for any unusual payments that you do not recognise, or if amounts you are expecting are not received.

21. Do I need to change any or all of my passwords?

Your passwords will not have been impacted by this cyber-attack. However, you should remain vigilant in applying any passwords. If you use online services or telephone banking, always use strong passwords, and change them regularly. Passwords should be as long as possible, using 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).

The National Cyber Security Centre offer this advice regarding choosing passwords, and is useful where retailers/business do not insist on the inclusion of numbers and special characters:

https://www.ncsc.gov.uk/collection/top-tips-for-staying-secure-online/three-random-words

22. Should I notify anyone of this data breach?

At this stage, the most important thing you can do is to be vigilant. We also recommend you sign up to Experian Identity Plus - full details of how to do this and your unique activation code can be found in the earlier letter to you from the Trustees.

23. To whom should I report any suspicious activity?

The Experian Identity Plus services offers guidance and support on how to report suspicious activity. We recommend you make use of the offer from Capita and sign up to this if you have not already done so.

The National Cyber Security Centre has lots of useful advice for steps you can take if your data has been accessed or used without your consent at the following website:

https://www.ncsc.gov.uk/guidance/data-breaches.

24. What else should I do to protect my data and my identity?

There are number of measures we can all take to keep us and our data as safe as possible:

- We recommend that you sign up for the Experian Identity Plus service - full details of which can be found in the earlier letter from the Trustees.
- It's good practice to keep an eye out for anything unusual in your email inbox or arriving by post.
- Be aware of what post is arriving at your home address, make sure you recognise any lenders contacting you and report anything suspicious.
- The most important thing is to stay vigilant and The National Cyber Security Centre has lots of useful advice for on next steps you can take if your data has been accessed or used without your consent.

25. How can I check to see if anyone has used my personal details?

To help you to monitor your personal information for signs of potential identity theft, Capita offered you a complimentary 12-month membership to Experian Identity Plus. This is a free credit and web monitoring service, provided by Experian, one of the UK's leading Credit Reference agencies.

This service helps detect possible misuse of your personal data and provides you with identity monitoring support, focussed on the identification and resolution of identity theft.

If you wish to take advantage of this free service, this will need to be activated by you. Details of how to activate this service were provided in the earlier letter to you from the Trustees.

You should note that, when you first activate the Experian Identity Plus service, Experian completes an eight year review and also reviews anything referenced on the web over that period. As such, the first return from Experian will show anything relating to that eight year period.

If you have not already subscribed to this service, the Trustees recommend that you should do so.

26. The Experian Identity Plus service was only being offered free of charge for 12 months. Have the Trustees negotiated an extension to this service for a longer period?

The free 12-month subscription to Experian's Identity Plus product was offered by Capita to all of its pension scheme clients for whom individuals were potentially impacted by this cyber-incident.

The Trustees raised their concerns with Capita over the duration of the free Experian access and initially secured a 12 month extension for members who have subscribed to this service.

The Trustees have since negotiated a further three-year extension to this free subscription with Experian, meaning that your free subscription will be for a total of five years.

At the end of the initial 12 month activation period, Experian will run an update in the background that will automatically update your service period from 12 months to five years. It is not expected that any further action will be required by you, this does not impact the use of the service, and no interruption should be experienced whilst this update is made. If you do experience any problems at the end of the 12 month period, please contact Experian using the contact information below.

27. Why is it that only the Experian service that has been offered? There are other credit agencies as well (such as Equifax).

Experian is the support product offered by Capita. Experian is a well-known and credible provider that has a significant share of the credit verification market in the UK and, more importantly, has access to the full credit market in the UK.

28. I already have an account with Experian for credit checks. What should I do?

Please contact the Experian helpline on 020 8090 3696, open Monday through Friday 08:00 – 18:00. You may be required to quote your unique activation number and other personal information to confirm your identity.

29. What should I do if I need to apply for credit? Do I need to unlock the Experian CreditLock before making an application?

Yes, you would need to unlock this before making such an application. Full details on the benefits of CreditLock and clear guidance on when and how to use it can be found on the Experian Website.

30. Is the Experian database safe? Should I be concerned about providing my personal data to Experian?

We are unable to comment on the security of national services such as Experian and other agencies. Experian has assured Capita that any personal data held on its servers is secure, and providing personal data to Experian is optional.

31. What should I do if Experian tells me that my data has been made available on the dark web?

We recommend you use the CreditLock feature which is provided as part of the Experian Identity Plus service, which means that people should not be able to apply for credit in your name.

Experian will provide further guidance to you on what actions you should take if it is found that your data does become available on the dark web.

The National Cyber Security Centre has lots of useful advice for steps you can take if your data has been accessed or used without your consent at the following website:

https://www.ncsc.gov.uk/guidance/data-breaches.

What steps are the Trustees taking against Capita?

32. Are the Trustees considering moving the payroll and administration services away from Capita?

The Trustees continue to monitor all of their suppliers in relation to all associated risks, including cyber security. In view of this incident, the Trustees have commissioned a third party to complete a review of Capita's security processes and, in particular, to understand what enhancements Capita has made to ensure the protection of the members' personal data.

As a result of the recent cyber incident, the Trustees are exploring all legal remedies against Capita and are considering the ongoing commercial relationship with Capita. This is commercially sensitive information and further comments are not available at the current time.

33. Are the Trustees holding Capita to account for this failure?

The protection of members' personal data remains the Trustees' top priority.

The Trustees' key focus at present is to work with Capita to ensure that all members' data is safe, and to work with the ICO and the Pensions Regulator on the impact of this data incident. As already stated, the Trustees are considering the ongoing services being provided by Capita to the Schemes.

I don't recall that I was a member of either of these Schemes. Were they previously known as something else?

34. What was the Sopra Steria Retirement Benefits Scheme previously known as?

The Sopra Steria Retirement Benefits Scheme was established when the following three separate legacy pension schemes merged together (the Steria Retirement Plan, the Steria Management Plan, and the Steria Pension Plan).

These legacy schemes have been through a number of iterations over the years. For example, the Steria Retirement Plan may have been known as the Bull Information Systems Limited Retirement Plan or the Honeywell Retirement Plan whilst you were an active member of the Scheme.

Similarly, the Steria Pension Plan may have been known as the Xansa Pension Plan or the FI Group Pension Plan whilst you were an active member of the Scheme.

35. What was the Steria Electricity Supply Pension Scheme previously known as?

The Steria Electricity Supply Pension Scheme was previously known as the Information Systems Electricity Supply Pension Scheme.

Who should I contact if I have any queries?

36. Who should I contact if I have any concerns?

- If you have any specific queries relating to the Experian services being offered, you should contact Experian directly using the helpline number of **020 8090 3696**, open Monday through Friday 08:00 – 18:00.

- If you have any questions regarding this cyber-incident, please contact the helpline on **0800 229 4005**, Monday to Friday – 08.30 to 17.30 and Saturday – 09.00 to 14.00. Please note that this helpline is provided by Experian.

- If you wish to raise your concerns about this cyber-incident with the Trustees, they can be contacted by email at pensions@soprasteria.com, or by post at the following address:

  Sopra Steria (Retirement Benefits Scheme) Trustees Limited / Steria Electricity Supply Pension Trustees Limited
  Three Cherry Trees Lane
  Hemel Hempstead
  Hertfordshire
  HP2 7AH

- If you have any other queries relating to your benefits under the Schemes, you should contact Capita by emailing steria@capita.co.uk, by calling **0330 3115119**, or by writing to the following address:

  Sopra Steria Retirement Benefits Scheme
  c/o Capita Pension Solutions
  P O Box 555
  Stead House
  Darlington
  DL1 9YT