CAPITA CYBER INCIDENT – UPDATE JUNE 2023

Our UK-based policyholders might have seen recent media coverage stating that Capita, who provide pension administration services to some of CNP Europe Life's policyholders, has recently experienced a cyber incident which involved unauthorised access to its IT systems.

CNP Europe Life has been informed by Capita that this incident has unfortunately impacted the personal data of 335 individuals who were former members and dependants of certain Shell UK Pension schemes. All impacted individuals are being contacted by post by CNP Europe Life to reassure them that their pension policies are unaffected and to provide further details and guidance on what steps they should take to protect their data. If you have not been contacted within the coming days you have not been affected.

There is a possibility that the personal data which has been exfiltrated could be used for fraud, identity theft or to send malicious emails, although Capita has no evidence that information resulting from this incident has been misused or that it is available illegally including on any third-party websites. Individuals who have been affected are being offered a specialist fraud monitoring service provided by Experian, one of the UK's leading Credit Reference agencies, as a precaution. Membership will be paid in full at no cost to those impacted.

CNP Europe Life has been working closely with Capita to understand how its cyber incident occurred and to put things right. CNP Europe Life's own systems were not impacted at all by the incident.

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. CNP Europe Life DAC has also notified relevant regulators.

Protecting the data of the 390 pensions we secure is a responsibility we take very seriously. On behalf of Capita and CNP Europe Life, we would like to offer our sincere apologies for any concern that this incident may have caused.

What other steps can you take?

If you have been contacted by us with confirmation that you have been affected by the incident, then as well as making use of the service from Experian, we encourage you to stay alert for 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 and then contact the helpline on 0800 2294005, Monday to Friday – 8.30 to 5.30 + Saturday – 9.00 to 2.00.

Other helpful information is available at:

- 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

- 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.

Beware Phishing

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 offer 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.

We apologise for any inconvenience and concern this incident might have 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 those policyholders who are impacted. 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.