Lisa Harley

From: GCEO@uss.co.uk <USS@dotdigital-email.com>
Sent: 26 May 2023 10:47
To: Lisa Harley
Subject: An update on Capita's data breach

View in browser

An update on Capita's cyber incident
26 May 2023

Colleagues,

I wanted to provide an update on our ongoing response to Capita's cyber incident.

As I set out in my last update on 17 May, members are being given access to a leading identity protection service provided by Experian, free of charge.

For clarity, USS is the data controller in respect of this incident. Capita is the data processor. At this time, the only member data Capita have formally confirmed was accessed via their servers is: their title, initials, and name; date of birth; National Insurance Number, USS number; retirement date. As we have yet to receive the actual data set in question from Capita, all members are being given access to Experian's service.

We have started to send voucher codes by email to members for whom we hold a valid email address. Members for whom we don't have a valid email address will receive a code by letter.

We are monitoring demand on Experian's support services, and this will influence the pace at which our emails and letters will be issued, but we are aiming to have issued all the emails by 31 May.

We have not given Experian any member data. Should members choose to use the voucher, Experian will be responsible for handling their personal data - and members will need to agree to Experian's terms and conditions to this end.

The ID protection service will monitor activity based on the information members give to Experian. Members will therefore need to provide some personal details in the sign-up process so that Experian can match them with their credit record for identification purposes and set up the monitoring. Members may also choose to provide Experian with certain personal details for monitoring the web (including the 'dark web').

If a member thinks there has been any suspicious activity on accounts in their name, or anything in their credit record they don't recognise, they should contact the organisation concerned as soon as possible.

Members have been asking why we cannot do this on their behalf. We only have oversight of members' USS accounts. The monitoring service provides far more comprehensive protection for members across services and accounts members may use, but over which we do not (and

would not) have any oversight. This service also requires explicit consent to set up and provides direct alerts to members. We therefore cannot set up this service on behalf of members.

We have updated the information on our website, including additional Q&As that respond to this and other questions we have been receiving from members. We hope these will also help your own teams to respond to any questions your colleagues may have. We will continue to add to these as required.

More broadly, Capita have confirmed that they have taken extensive steps to recover and secure the data as well as monitoring the 'dark web'. While at present we understand from Capita that the data "exfiltrated" has been secured, we are also taking steps to put our own monitoring in place.

We continue to proactively engage with Capita in respect of their investigations and are keeping this incident (as a whole) under constant review.

Having reviewed our own systems and controls to ensure they remain robust, we are very confident members' pensions remain secure. My USS login information has not been compromised. We have strengthened our ID and verification processes and, purely as a precaution, taken our active member Benefit Illustrator offline.

I want to reiterate that we know our members will be concerned about this potential risk to their personal data, we very much regret that this has happened – and we are fully focused on supporting them through this issue.

Bill Galvin, Group Chief Executive