25 May 2023

Capita cyber incident - Q&As

Capita recently reported a cyber incident involving hackers targeting some of its computer servers – potentially impacting several of the cross-sector businesses it serves.

We use Capita's technology platform (Hartlink) to support our in-house pension administration processes and have been liaising closely with the company over the course of its forensic investigations.

While it has been confirmed that USS member data held on Hartlink has not been compromised, we were informed on Thursday 11 May that regrettably details of USS members were held on the Capita servers accessed by the hackers. Capita have since identified from their investigations that personal data was "exfiltrated" (i.e., accessed and/or copied) by the hackers. The information accessed includes:

> Their title, initial(s), and name; their date of birth; their National Insurance number; their USS member number and their retirement date

The details, dating from 2021, cover around 470,000 active, deferred and retired members.

Capita have confirmed that they have taken extensive steps to recover and secure the data as well as monitoring the 'dark web' to confirm that data compromised as a result of this incident is not circulating more widely.

Members are being given access to a leading identity protection service provided by Experian, free of charge, and we will be writing to them week commencing 22 May 2023 setting out how that will work.

We have published an update on the USS website and have provided the following Q&As, which we hope will address any immediate questions members may have. Members can also email mydata@uss.co.uk if they have any further queries not covered on www.uss.co.uk.

We are proactively engaging with Capita in respect of their ongoing investigations and are considering the next steps available to us.

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.

25 May 2023

Experian service-specific

How do I know the email I received from USS is genuine?

Please check the email address carefully. Our emails to members come from members@news.uss.co.uk

If you are concerned someone might be impersonating USS, please let us know by emailing mydata@uss.co.uk

I have not received an Experian voucher code. Does that mean my data has not been affected?

We are sending the voucher codes to all members in batches, over multiple days, in order to manage demand. We are emailing members for whom we hold a valid email address. Members we don't have a valid email address for 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.

The activation code hasn't worked

Please contact Experian's Customer Support Centre on 020 8090 3696. They are open Monday to Friday, 8am to 6pm. (Charges for calling 02 numbers are the same as calls made to a standard UK landline.)

I can't get through to the Experian Helpdesk

Please keep trying – a number of other companies have been affected by Capita's data breach and have offered this service so their contact centre is likely to be experiencing high volumes of calls.

Why do I need to provide my bank or card details?

You may need to provide Experian with some personal details in the sign-up process so that Experian can match them with your credit record for identification purposes and set up your monitoring.

Are the questions Experian asking expected as it's a lot of personal information?

If you choose to use the service, you will need to provide Experian with some personal details in the sign-up process so that Experian can match them with your credit record for identification purposes and set up your monitoring. You should review Experian's terms and conditions to make sure you are comfortable sharing the information requested.

25 May 2023

Is Experian covering all data that may have been compromised – like data that Equifax would cover for example?

Experian is one of the three main consumer credit reference agencies. They hold information relating to your credit, service and utility accounts.

What will happen when I input my details and follow the steps?

You will be guided through the process of setting up the Experian Identity Plus services after following the link in the email. If you require additional support, please can the Experian Identity Plus product helpdesk on 020 8090 3696. They are open Monday to Friday, 8am to 6pm.

(Charges for calling 02 numbers are the same as calls made to a standard UK landline.)

Why is the onus being put on members to monitor their personal information?

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 are proactively engaging with Capita in respect of their investigations and are considering the next steps available to us.

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.

But 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.

Does Experian now have my personal data?

We have not given Experian any of your information. Should you choose to use the voucher, Experian will be responsible for handling your personal data and you will need to agree to their terms and conditions to this end. Your voucher code lets you sign up for the Experian service free of charge. You will need to provide some personal details in the sign-up process so that Experian can match them with your credit record for identification purposes and set up your monitoring. You may then also choose to ask Experian to monitor the web (including the 'dark web') for certain personal details provided by you.

What happens if there has been activity between the date the hack happened and the date it was identified?

The ID protection service will monitor activity based on the information you give to Experian. If you think there has been any suspicious activity on accounts in your name, or anything in your credit record you don't recognise, contact the organisation concerned as soon as possible.

Why are you only providing this service for 12 months?

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 are proactively engaging with Capita in respect of their investigations and are considering the next steps available to us.

What should we do if our data is used to take out credit/loans etc?

The ID protection service will monitor activity based on the information you give to Experian. If you think there has been any suspicious activity on accounts in your name, or anything in your credit record you don't recognise, contact the organisation concerned as soon as possible.

Should I tell my bank?

This is something for you to consider, but we would suggest it is only necessary if you think there has been any suspicious activity on your account.

General

What member data has been taken?

The details, dating from 2021, cover around 470,000 active, deferred and retired members. We understand this data is contained in files generated by Capita from the main Hartlink system, and held separately on Capita services, to facilitate operational processes. Capita have identified from their investigations that personal data was "exfiltrated" (i.e., accessed and/or copied) by the hackers. The information accessed includes:

> Their title, initial(s), and name; their date of birth; their National Insurance number; their USS member number and their retirement date

How many members are affected?

The details, dating from 2021, cover around 470,000 active, deferred and retired members. While we await receipt of the specific data from Capita, we have arranged for all current members of the scheme to have access to a leading identity protection service, free of charge.

25 May 2023

When were you first made aware that USS member data had been affected?

We have been engaging closely with Capita since it first announced the cyber incident. Capita first formally informed USS of a personal data breach on Thursday 11 May 2023.

How quickly did you let members know?

Within a day of formally being informed, we published an update and an initial set of Q&As (available via the www.uss.co.uk homepage) to address immediate questions – and began to email members. We will be writing to each of the members affected by this – and, where applicable, their employers – as soon as possible to make them aware, to apologise for any distress or inconvenience caused, and to provide ongoing support and advice.

How are you protecting the members affected?

We are proactively engaging with Capita in respect of their ongoing investigations and are considering the next steps available to us.

Capita have confirmed that they have taken extensive steps to recover and secure the data as well as monitoring the 'dark web'.

Members will be given access to a leading identity protection service provided by Experian, free of charge, and we are writing to them setting out how that will work.

What advice can you give to affected members to protect themselves?

We would encourage members to only ever give out personal information if they are absolutely sure they know who they are communicating with.

- If you receive a suspicious email, you should forward it to report@phishing.gov.uk
- For text messages and telephone calls, forward the information to 7726 (free of charge).
- For items via post, contact the business concerned.
- If there are any changes to your National Insurance information, HM Revenue & Customs would contact you – but you can also phone them on 0300 200 3500.
- If you are concerned someone might be impersonating USS, please let us know by emailing mydata@uss.co.uk

The National Cyber Security Centre and the Information Commissioner's Office (ICO) both provide guidance that may also be useful.

On what grounds can we be sure Capita are addressing this incident robustly?

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.

25 May 2023

What is being done to ensure pensions and other data remain secure in the long term?

We want to assure members that data privacy and security is a top priority for us.

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.

We use Capita's technology platform (Hartlink) to support our in-house pension administration processes. While it has confirmed that USS member data held on Hartlink has not been compromised, regrettably details of USS members were held on the Capita servers accessed by the hackers. We understand this data was contained in files generated by Capita from the main Hartlink system, and held separately on Capita services, to facilitate operational processes.

Can someone call using the info copied and change the bank account my pension is paid into over the phone?

They would not be able to do this, as a person contacting USS to make changes to a pension would need to know additional information.

Is my USS online account safe?

Yes, this is a personal data breach and not a breach of My USS login information.

Are my investments and pension safe?

We are confident members' pensions remain secure. We have reviewed our own systems and controls to ensure they remain robust. My USS login information has not been compromised.

Have you informed the Information Commissioner's Office (ICO)?

Yes, we have reported this to ICO and will work with them on any investigation they choose to conduct and any recommendations they might subsequently make to USS.

Have you informed UCU and UUK?

Yes.

Have you informed The Pensions Regulator?

Yes.

25 May 2023

Have you informed the Financial Conduct Authority?

Yes.

Are you carrying out your own checks?

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.

How are you going to compensate members if somebody commits ID fraud using the details that have been accessed?

We are proactively engaging with Capita in respect of their investigations and are considering the next steps available to us.