Capita Cyber Incident

Questions and answers

You'll be aware that Capita provide the administration services for EAPF members' pensions. On 31 March 2023, Capita detected malicious activity on their networks, and we've set out below some questions you might have about what this means for former members impacted by the incident.

1.0 The Incident, the data and what it means

1.1 How did the cyber incident occur?

The cyber incident occurred at Capita plc, and it impacted a small number of its computer servers. This included some used by Capita Pension Solutions, which is a business that provides pension administration services to members of the EAPF, along with several other major pension schemes.

1.2 When did it happen?

The initial malicious activity took place on 22 March 2023. Capita detected the activity on 31 March 2023 and intercepted it immediately.

Since then, Capita have undertaken a complex forensic investigation with support from technical experts and specialist advisers. This has involved reviewing files across their entire business.

1.3 Why did it take Capita 9 days to identify the malicious activity?

Unfortunately, it's not unusual in cyber incidents for the attack to remain undetected in an IT estate for long periods, sometimes months. Being quietly undetected allows the cyber criminals to scout out the business before seeking to further their criminal activities.

However, the unauthorised intrusion was interrupted by Capita in this case in less than 9 days. Capita's action resulted in the impact of the incident being restricted significantly. The investigation following this was complex and needed to be comprehensive to identify if any data had been exfiltrated during the 9-day period where the attack went undetected.

1.4 When were you first made aware that my data had been affected?

We've been working closely with Capita since it first announced the cyber incident and have sought regular updates on the progress of its investigation. Once Capita had confirmed there was evidence that some personal data may have been accessed, we updated the EAPF public website. At this point, they were unable to confirm whether members or former members' personal data had been affected.

We were formally informed of a personal data breach specifically for certain pensioner members in the Scheme late in the afternoon on Friday 19 May. At this point, the full forensic analysis was not complete.

Nevertheless, we updated the website during the following weeks before being in a position to write out to those we believed to be affected in early June.

We've since received the full, final forensic investigation results which confirms the data that was available for our members and former members.

We've worked as quickly as we could to review the data in order to write to those affected setting out exactly how they have been affected.

1.5 Why has it taken so long for you to write to me?

The full forensic investigation was completed by Capita and shared with the EAPF in mid-June. We wrote to many members we had the relevant information for in early July.

Unfortunately, due to the need to confirm former members are 'living as stated' it has taken longer to be in a position to write to this group as the tracing exercise takes a number of weeks. We have written to you as soon as we practically could.

1.6 What does 'exfiltrated' mean in the context of this incident?

The definition of 'exfiltrated' in a cyber security context is:

- The unauthorised transfer of information from an information system

1.7 For some of the data fields in my letter, I'm not clear on what they actually mean – can you clarify?

Following an earlier mailing, we received many queries on data fields and so we asked Capita to set out a data definitions table which is included below:

Data Item	Description:
Address	Home Address
DOB	Date of Birth
Email Address	Personal or work email address
Employment Details and History	Dates of employment, job role, date of leaving company
Expression Of Wish Details	Names, addresses and relationship to those nominated as beneficiaries for benefits payable on death
Gender	Male/Female (may have been inferred from TITLE)
HMRC Data	Usually Tax code, could also be tax deductions, employer PAYE reference
Location Data	Current or previous employment location (for dependants this would relate to the member)
Maiden Name	Maiden Name
Marital Status	Marital Status
Name	Title, initials, forename and surname or a combination of these
NI number	National Insurance number

Data Item	Description:
Online Identifier	A pension website login name or an indication that the member has an online account (usually EAPF Online)
Postcode (Area Code)	The first part of the post code (may be duplicated in address)
Postcode (Full)	The whole postcode (may be duplicated in address)
Spouse Details	Name and/or date of birth and/or address. Gender could be implied from title in the name
Bank Details	Full Sort Code and/or account number (redacted entries e.g. "2*****32" would not be flagged) – see question 1.10 for further info
Pension Details and History	Gross/Net Pension, pension contribution, fund value or lump sum amounts, AVC pot value, transfer amount quoted or paid, estimated benefits
Salary	Gross or pensionable salary
Sexuality	This is not a data field Capita holds, however, it may be included in a letter where the ICO has determined that from other data available it could be possible to assume your sexuality. For example – marital status and spouse details.

Please note the above table includes the full list of data fields that could have been exfiltrated – however, the fields that apply to you are solely those listed in your individual letter.

1.8 What could someone do with this data if it is sold online? What are the risks to me?

It's important to note that to date, it remains the case that there is no evidence that the data has been sold or leaked on the dark web, which Capita are continuing to monitor closely through third party experts. Capita have set out that the risk is the potential for identity fraud in the event that data is misused.

Identity fraud could take the form of: trying to open an account in someone's name/ making a purchase in someone's name/ using someone's personal details in criminal activity such as using fake details for car insurance, etc.

In order to reduce these risks, they recommend registering for the Experian service in addition to vigilance in the form of looking out for suspicious emails and using caution in clicking on links without verifying it's from a reliable source.

1.9 How long will the third party expert continue monitoring the dark web for signs of my data being sold or misused?

Capita's agreement for this monitoring is currently open with no cessation, they don't have a view at present as to when this will end.

1.10 It says that bank details were exfiltrated as part of this attack. Why do you hold bank details for me?

It's possible that the bank details held are not actually linked to you. This depends on whether you received a refund of your EAPF contributions, or if the pension you held in the EAPF was transferred to another provider.

If you received a refund, then the bank details held are likely to be for the bank account the refund was paid in to. If your former EAPF benefits were transferred to another provider, it's likely that the exfiltrated bank details are from the receiving scheme your EAPF benefits were transferred to. Capita have taken a cautious approach with this exercise, and so if any bank details were noted with your details, it will be stated that bank details were exfiltrated in the letter provided to you.

1.11 What can attackers do with bank details?

There is actually little someone can do with just an account number and sort code, aside from making a deposit into the account. These are the details we give people when we want them to pay something into our account.

To pay for things online, you would need things such as the long card number, expiry date on the card, and name of the account holder and the CVC code. However, organisations can set up direct debits to make payments with just an account number and sort code.

We understand that only companies that have been vetted by the Direct Debit Scheme can use an account number and sort code to take money from an account in this way, and the funds are always protected by the Direct Debit Guarantee.

With an account number and sort code, scammers may also be able to identify your bank and try and send you emails pretending to be your bank, however - this would be on the sophisticated side of scams.

For your peace of mind, we would recommend registering your free account with Experian if you haven't already. There is the option to add your bank account details/credit card details to specifically monitor some or all of your accounts. You can also activate a 'Credit Lock' which means that this would have to be unlocked on the Experian account in order to apply for credit in your name.

It is a personal choice if you wanted to go even further and contact your bank to discuss this to see whether it would be wise to change account details. But this should not be necessary as the Experian service is deemed to provide sufficient monitoring for you.

1.12 Does the fact you have my details mean I still have a pension in the EAPF?

No. The reason Capita have retained your details is for compliance with GDPR.
See 1.13 for further information.

Often, Capita receive contact from, or in relation to, former members at their retirement or death to confirm whether benefits are held. This means retaining some data can enable Capita to confirm whether their pension rights were refunded or transferred elsewhere.

1.13 Why does Capita still have my information when I don't hold a pension in the EAPF any longer?

Capita provides pension administration services to a number of businesses including the Environment Agency Pension Fund (EAPF). In order to provide these services, certain data was shared by EAPF with Capita.

Capita has a Data Retention Standard which mandates how long records, including personal data, must be retained. Capita will retain your personal information for as long as necessary to fulfil the purposes Capita collected it for, including for the purposes of satisfying any legal, accounting, tax, regulatory or reporting requirements. For this reason, details of those who no longer hold pension benefits in the EAPF have been retained in Capita's systems.

1.14 Does this impact all members and former members?

Not all, but we now know that all member types are affected and higher numbers than we were initially informed of. The information potentially accessed does vary for each individual and has been set out in their individual letter.

1.15 Is Capita certain that the personal data found on the files has been accessed?

Capita cannot be certain that the personal data has been accessed. You can read Capita's full statement here at **www.capita.com/news/update-actions-taken-resolve-cyber-incident**

1.16 What advice can you give to members and former members who are concerned?

In a data-driven world, we always recommend taking steps to protect your personal data and avoid scams. We'd encourage you to only ever give out personal information if you're absolutely sure you know who you're communicating with.

- **Do not click on any links included in emails** unless you know it is from a reliable source.
- **Do not provide any personal information** unless it is a request from the administration team that is in direct response to an enquiry from you.
- **Use your mouse to hover above the email address to check its origin,** if the email is from a third party pretending to be someone else, you might spot this by holding the mouse above the email address. If anything looks unusual (perhaps a spelling discrepancy or uses numbers in place of letters), it's best to verify the email address through the organisation's website.
- **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.

2.0 Regulatory questions

2.1 What are your legal and regulatory obligations?

We are required to inform the Information Commissioners Office (ICO) and the Pensions Regulator (TPR) about the incident. We have reported the impact to the Fund to both ICO and TPR and will work with them on any investigation they choose to conduct and any recommendations they may make.

2.2 Should I also contact ICO even though you have?

There is no need for affected individuals to contact ICO as they are already aware of the data breach and have been provided with regular updates for the EAPF and Capita.

2.3 Is there any guidance available from a regulatory perspective?

The National Cyber Security Centre and the ICO both provide guidance that may also be useful. You can visit their websites using the below web addresses:
www.ncsc.gov.uk/guidance/data-breaches
ico.org.uk/for-the-public

2.4 How will you make sure that this doesn't happen again?

In our discussions with Capita, we have sought information about what has been done to improve the security of personal data and avoid a future incident. Now that the investigation has been finalised, we're awaiting a full report about the incident, how it was managed and what steps Capita has taken and will be taking to avoid this happening again.

2.5 All of this data should have been segregated and encrypted - was this not the case?

Some of the data was encrypted, but sadly not all. EAPF has written to you because at least some of the information Capita handles on behalf of EAPF was not password protected or encrypted.

This is a matter that will be addressed by the ICO and TPR determination following their investigations into the incident. We are hoping that more information on why not all the data was encrypted will be clarified in their investigation report.

We appreciate that this will be a concern to you, and we understand your frustration.

Capita has appointed a third-party specialist adviser who continues to monitor the dark web to confirm that data compromised as a result of this incident is not available for sale online.

Further, Capita have assured us that they are continuing with their multi-year investment programme focused on ensuring the integrity of its cyber-security environment. However, unfortunately, no entity can assure themselves they will never experience a cyber-incident.

2.6 Will Capita give me compensation for the distress the incident has caused me?

We are in discussions with Capita on the compensation that's been offered to members (the 24 month Experian service) with a view to have further support in place. We're also in regular contact with the other impacted pension funds, as part of Capita's large client forum. As you can imagine, we are all keen to progress this as quickly as possible, but the scope of the incident is vast, so the reality is that it is going to take some time.

In addition to this, the incident has been reported to both the Information Commissioners Office and The Pensions Regulator. At this stage, it is too early for us to know what the Information Commissioners Office (ICO), the Pensions Regulator (TPR) and other regulatory bodies will determine for Capita. Once this has concluded, a judgment will be delivered which could result in a review of the compensation offered. This judgment may take several more months and until this is completed, we are limited in being able to advise what the outcome may be.

3.0 The Experian service

3.1 Who are Experian?

Experian are a trusted, leading identity protection service who specialise in the protection of data. This service helps detect possible misuse of your personal data and provides you with identity monitoring support, focused on the identification and resolution of identity theft.

3.2 How does the Experian service work?

This service notifies individuals via email or SMS when their personal information has been found on the web.

3.3 My Experian code doesn't seem to be working, what can I do?

Unfortunately, the EAPF branded font has made the letter 'I' look like a number '1'. Most commonly, the beginning part of the code should be 3 letters for e.g. CPI and many have been incorrectly trying CP1.

If this doesn't fix it, you may need to contact Experian by phone on Tel. 020 8090 3696 They're open Monday to Friday between 8am to 6pm.

3.4 What information will Experian ask for?

The following information is compulsory for Experian to set up the service:

- Name
- DOB
- Address (current and one previous)
- Email address
- Password creation

At this point, a verification process will take place. Given the level of sensitive information contained within a Fraud Report, this process involves checking that the person registering is who they say they are.

On completion of the verification process, you will receive a welcome email and will be able to enter any additional information that you would like to be monitored including who you bank with if you wish.

3.5 How can Experian help me to protect myself from fraudulent activity?

The Experian service provides you with access to your Experian Fraud Report where you'll be able to view alerts and certain changes, such as a loan application. Individuals will also be alerted via email of personal information found on the web via our web monitoring service. This vital insight can help you to determine if you're at risk of becoming a Victim of Fraud.

3.6 How can Experian help me if I am impacted by fraudulent activity?

If you don't recognise changes to your Experian Fraud Report, you can contact Experian by calling their call centre or completing an online enquiry form.

A member of their Victims of Fraud Resolution Specialists can open and review your case. They will work with you to advise on the appropriate next steps. This may involve adding a CIFAS Protective Registration flag to your Experian Credit Report. In the future, this preventative measure can help if any further applications are made to a company who is a CIFAS member. They may contact you to carry out additional checks on the application to determine if it is genuine and not an attempted identity theft.

3.7 How do I register for the Experian service?

Affected individuals will receive a letter containing a unique voucher code which can be used to register for the free 24 month membership. The letter explains the steps to follow to access this service. There is also a contact number so you can speak directly to Experian if you have any questions.

Please note - on registration, the membership expiry date will initially be displayed as 12 months' service. This is because 12 months was the original offering which has since been extended to 24 months. This will be updated to reflect 24 months' service automatically by Experian **within 90 days of the activation code expiry date** provided within your letter. This won't impact the use of the service and no interruption will be experienced whilst the update is made.

3.8 How do I activate my code if I'm already registered to an Experian 'free' account?

If you were already registered to an Experian `free' account before this incident and need some help activating your code for Experian `Plus', we've added some guidance that you can download to help you at **www.eapf.org.uk/cyber** (and click the box called `Q&A for UK members').

3.9 Will Experian ask for my bank details?

Experian will ask who you bank with as part of the verification process. This will ask you to choose from a list of potential banks and the same for who you may hold a credit card with or may have a loan with.

However, it is optional to add specific account details if you'd like these accounts to be monitored in addition for financial interactions that could be fraudulent. In very limited cases, Experian may ask for card information if they are unable to verify the identity of an individual.

3.10 What else can Experian do to protect me?

When you register, you have the ability to activate a `Credit Lock' facility free of charge. This significantly reduces the chance that credit can be applied for in your name.

It does also mean that if you are applying for credit yourself, in order to be successful, you will need to remember to `unlock' this facility. If you leave the Credit Lock activated when applying, with some lenders it will take 30 days before you are able to apply again.

3.11 I've registered for Experian and it shows that my details are being sold online! How can this be when Capita say there is no evidence that this is the case?

We recognise the significance of the concern our members and former members in this situation will have. However, as already confirmed, Capita have stated the following:

"Capita has appointed a third-party specialist adviser who continues to monitor the dark web to confirm that data compromised as a result of this incident is not being circulated or available for sale online. They have been appointed since the earliest days of this incident. The third-party reports to Capita that they can find no evidence of data resulting from this incident being circulated online or available for sale on the dark web or otherwise."

With the Experian service when you first set up your account, they run an initial check of your details over an 8 year period. This means they will notify you for any instances your details have appeared online over the past 8 years. This means that the alert could be from a separate instance over the past 8 years, as to this date, the continuous monitoring of the internet and the dark web by third party experts has not identified evidence that data exfiltrated in the cyber incident has been sold or leaked online.

If you wanted more information on an Experian alert you've received, there is a dedicated phone line to help those who have questions or concerns about this. We'd recommend calling Experian on **020 8090 3696** to see if they can provide more information.

3.12 I've recently received a lot of phishing emails – are these related to the Capita cyber-attack?

Capita's third-party specialists have yet to find any evidence that the exfiltrated data from the cyber-attack has been sold or leaked on the dark web. These specialists are continually monitoring the dark web, but nothing has been found to date. However, it may provide peace of mind to use the Experian support on offer. If there was anything untoward happening to your personal email address online, the activity would be flagged via Experian. Any concerns you may have can be raised with the support team on hand.

During this time, please remain vigilant and don't click on any of the links or attachments from these phishing campaigns. You have the option to report such campaigns to **report@phishing.gov.uk**, plus you can report these messages as junk or phishing to your email provider by using the 'report message' option on the toolbar.

If using a Gmail account, there is an option to click 'Message looks suspicious', which prompts the Gmail team to investigate. Furthermore, you can block the sender to try and prevent any more emails coming through.

Further advice can be found on the NCSC website: **www.ncsc.gov.uk/collection/phishing-scams**

3.13 Is the 24 months Experian membership enough? The data can be out there forever for criminals to use.

We do appreciate the concern around your data being exfiltrated and the unknowns and uncertainty of what will happen with this in the future. Capita had advised that 12 months was appropriate for this type of incident – and this was initially offered to those affected by the incident.

However, as a management team we acknowledge and understand that to many, 12 months didn't seem enough. On 2 August, it was agreed for the 12 month free membership of Experian to be extended to 24 months.

Please note - on registration, the membership expiry date will initially be displayed as 12 months' service. This is because 12 months was the original offering which has since been extended to 24 months. This will be updated to reflect 24 months' service automatically by Experian **within 90 days of the activation code expiry date** provided within your letter. This won't impact the use of the service and no interruption will be experienced whilst the update is made.

3.14 What will reduce the chances of becoming a victim of fraud?

When you register with Experian, if your fraud report identifies fraudulent activity, the Experian service will create a flag with the Credit Industry Fraud Avoidance System (CIFAS). CIFAS is used by most organisations when credit is applied for.

This flag identifies you as a person who has been subject to identity fraud, which will significantly reduce the risk of further identity fraud. This is because if credit is taken in your name going forwards, you will be contacted to verify that the credit application is genuine.

3.15 Do I need to contact anyone (e.g. bank etc) to let them know this has happened?

Once you are set up with Experian, they will alert you to anyone you may need to get in touch with.

Whilst there is no need to contact any organisations you are linked with unless fraudulent activity is detected, the decision to contact your bank is a personal one and may be prudent.

3.16 I'm unable to register my Experian membership as my IT skills/access to IT is limited, so what should I do?

This was a digital incident, the only inclusive ID monitoring service available to members is a digital offering from credit bureaus such as Experian. The service has been recommended to Capita by third-party experts as the most appropriate and immediate way of supporting those affected at this time, so that the potential impact of the incident is minimised.

In order to sign up for the Experian service you will need access to the internet and an email address. However, we understand that not everyone will have internet access.

Getting help from someone else
It is possible for others to create and monitor an Experian account on your behalf (for example, a family member or a trusted third party).

If your Experian account is created and monitored by someone else and they want to contact Experian on your behalf, they will ask for evidence that:

- you have provided your consent for your representative to contact them on your behalf (e.g. by asking to speak to you); or
- they have Power of Attorney, Deputyship or similar legal authority where you're unable to provide your consent for them to contact Experian on your behalf.

If you have further questions on this, you should call Experian on **020 8090 3696** (open Monday to Friday, 8am to 6pm). Their advisors understand the service and how it works.

If you don't have internet or anyone else to help you register
Experian, like all other providers of the credit monitoring services in the UK, only offer an online service, due to the nature of how individuals are verified and also the types of information that is required to be entered, if you wish to use the service to its full potential.

Therefore, the only 'offline' service they provide is a one off Statutory Credit Report of your credit file. The application can be made by post or online. This is offered free of charge and as it's a 'one off' report, it doesn't monitor against fraud.

You can call Experian for more information about this report on **020 8090 3696**.

3.17 What if I have other questions not covered here?

We've done our best to cover as many questions as possible and have updated and added to these following further queries raised from previous mailings.

We'd urge you to set up your Experian service and contact them if you have questions. If you have other questions that you want to ask Capita, please be patient with the team. The incident has had an impact on their 'business as usual' processing.