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 have set out below some questions you might have about what this means for our members.

We have updated this Q&A on 10 October 2023. The Q&A is now split this into clear sections.

1. The incident and what it means – new questions 1.5 and 1.8-1.12
2. Regulatory questions – new questions 2.7-2.9
3. The Experian service – new questions 3.10- 3.11, 3.13, 3.16 and 3.18. Updates have been made to 3.7 and 3.12 (regarding when the Experian code will update to 24 months).

The additional new questions listed above were not available at the time your printed letter was issued.

1.0 The Incident, the data and what it means to members

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 When were you first made aware that member 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 members on the EAPF public website. At this point, they were unable to confirm whether 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. Before the letters were sent, we emailed these members (where email addresses were available), to inform them of the breach and that a letter would follow. Large mailings take time and planning and we had to ensure all our messages were clear and timely.

We've since received the full, final forensic investigation results which confirms the data that was available for our members. We've worked as quickly as we could to review the data in order to write to all affected members setting out exactly how they have been affected.

1.4 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. There are a lot of steps required to produce a large, printed mailing that provides information specific to each individual. This takes a minimum of 7 working days, and we also wanted to make sure you had additional information in the form of the Q&A.

We felt it was important to line up all the appropriate communications needed both internally and externally. Our communications plan has factored in the timescale for the mailing as well as the timing of messages to ensure both we and Capita would have a better ability to respond to queries considering we are only a small team. Please do bear with us if you have to get in touch.

1.5 Can I receive a copy of the letter sent to me on 6 July?

A copy of your letter has now been uploaded to EAPF Online account.

If you need to reset your EAPF Online pin or password or need a reminder of what you chose as your login name, there are a number of ways you can do this below.

- **Use our self-service Reminder facility** at **portal.eapf.org.uk** (see bottom left corner of the homepage)
- **Complete our secure online contact form** at **www.eapf.org.uk/ask-us-a-question**
- **Telephone our contact centre** on 0800 121 6593
- **Email eapasswordreset@Capita.com**

If you choose to email the request, please note you'll need to provide the below information in order for the team to access your account.

- Full Name
- Your National Insurance Number
- 1st line of address
- Date of birth

Then one of the below pieces of information:

- Date Joined Employer
- Date Joined Scheme
- Date Left Scheme
- Normal Retirement Date
- Payroll Number

1.6 What personal data has been accessed in the incident?

Regrettably, details of EAPF members were held on the Capita servers accessed by the hackers. We've written to those EAPF members who have been impacted, setting out the precise categories of personal data impacted.

Whilst Capita has informed us that there is no evidence that information resulting from this incident has been misused, Capita believes it is appropriate to act with vigilance under the circumstances.

1.7 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

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

Following the mailing, we received many queries on data fields. 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	NI Number
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)
Data Item	**Description**

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 hold, 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 letters.

We believe that the exfiltrated data file captured a moment in time historically because we know that newer members of the scheme did not appear on the file. Therefore, some of the data items are now likely to be out of date (for e.g. salary or job role). At this point in time, we do not know the date the data was captured.

1.9 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 a third party expert. 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 the risk to members, 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.

1.10 My bank details were exfiltrated as part of this attack. What can attackers do with these? Should I change my bank account?

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. Lots of small businesses will also have account number and sort code on their business cards to allow customers to pay them.

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. Although, 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.

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.

1.11 My spouses and/or Expression of Wish nominee's details were also exfiltrated. Will you provide an Experian code for them?

Capita have only provided Experian codes for members who are impacted as they consider that the risk of fraud is significantly reduced due to the limited data available for a spouse/expression of wish nominee. However, please see the response to questions 2.9 and 3.12 regarding the EAPF's position on this.

1.12 The exfiltrated data states 'Email address' but I don't know which one this is?

For active (contributing employee) members, Capita will automatically have your EA or NRW email address. If you added another email account when registering online, and set this as your preferred email address, Capita will have both your EA/NRW email address and your preferred email you have added.

For all members, the email address included in the exfiltrated data is most likely to be the preferred email address you have set up for your online services.

1.13 Is my pension safe?

We'd like to reassure all members that your pension benefits remain secure. Hartlink, the database that holds all member pension records, was not impacted by this incident. The main advice we can provide is not to be alarmed, but to be vigilant given the circumstances.

We have set out some recommendations in question 1.18 below.

1.14 Has this affected pension payments made to members?

All pension payments have and will continue to be paid on time.

1.15 Does this impact all 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 letters.

1.16 Have you contacted all affected members?

We have written to all members who have been affected by the incident. There are however, a small group of members that we've been unable to contact due to no address being held on file and some members who are no longer part of the scheme. We have also updated members internally and via the Fund's website confirming details of the incident.

Letters have also been added to members EAPF Online accounts too.

The letter confirms the details of the information that was available on the affected

server relating to them. It also highlights the potential risks and the steps the affected members can take to protect their personal data. Capita have also provided free access to a service that Experian offers (called 'IdentityWorks') that will help members monitor the use of their personal data. This was initially set out to members for 12 months but was extended to 24 months on 2 August 2023.

1.17 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**

1.18 What advice can you give to members who are concerned?

Whether you've been impacted by this incident or not, in a data-driven world, we always recommend that members take steps to protect their personal data and avoid scams. We'd encourage all members to only ever give out personal information if you're absolutely sure you know who you're communicating with.

- **If you receive an email from the EAPF administration team**, please make sure the email is from a Capita email address (either @capita.com or @capita.co.uk).
- **If you receive an email from our Communications team**, please make sure the email is from **noreply@mail.eapf.org.uk**
- **If you receive an email directly from our EAPF Management team**, please make sure the email is from **@environment-agency.gov.uk**
- **Use your mouse to hover above an incoming 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.
- **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.
- **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're concerned someone might be impersonating EAPF, please let us know by emailing **info@eapf.org.uk**

1.19 Is my pension account on the EAPF Portal safe?

Yes, the portal was not accessed, and your login information remains safe.

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 members 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 Are and how are the unions being involved in this?

The trade unions have been kept informed of the situation and we'll continue to engage with the unions as and when we have an update on the forensic investigation results, and any information of interest to members.

2.5 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 are 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.

2.6 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. We understand that Capita have 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. 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. 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.

2.7 Who is accountable for the loss of my data?

The EA Board delegates the management of the Fund to a Pensions Committee. This is supported by officers from a Pension Fund Management Team who work within the Environment Agency.

Cyber Security has been a priority focus for the Pensions Committee for the last 3 years. This has included the approach of our key data processor Capita. (See Question 2.8 for technical details on this).

The EAPF, as data controller, continues to oversee actions to mitigate the impact on members, manage this complex and live incident and ultimately to assess liability. We are working with Capita, regulators, and some of the other 90 plus organisations affected by the cyber-attack.

2.8 I don't feel that the EAPF has done enough to protect me

We want to reassure you that Cyber risk has been a priority on our agenda over recent years and we take our responsibility for protecting our members data extremely seriously. We do share your concerns as our contract with Capita included that they should implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk; including the encryption of our personal data.

During the procurement process, we work alongside Defra's procurement team to ensure the onboarding of new suppliers is robust and compliant with Defra's standards.

Cyber Security has been a priority focus for the Pensions Committee for the last 3 years. The Fund has taken many actions to mitigate cyber risk, including the use of external specialists to assess the cyber security credentials of our key suppliers. The external security specialists leveraged their expert knowledge across multiple cybersecurity frameworks, standards and industry-best security practices, and created detailed questionnaires. They reviewed the answers to provide a high-level view of the maturity and effectiveness of the security controls of our key suppliers.

One of these assessments focused on Capita's approach to cyber security.

Capita answered just under 150 questions on different security domains, including "Security Governance" 'Data Security' and 'Access Controls.' In Capita's assessment, we were assured that they adhered to multiple international Standards, including ISO 27001. While we cannot release the completed report due to the document being commercially sensitive, we can summarise that the report concluded in 2022 that Capita's approach in these areas clearly evidenced good security best practices. No security domain required immediate further action.

While no entity can fully protect itself from the ever growing and ever changing threat of cyber crime, the assurances the EAPF sought from Capita concluded that the security controls in place were in line with best practice.

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

We are in discussions with internal legal representatives, external legal advisors and Capita on the compensation Capita have offered to members (the 12 month Experian service which has now been extended to 24 months) with a view to have further support in place. As the EAPF is one of many pension funds that have been impacted by this incident, we are also in continuous discussions with other impacted pension funds as part of a large client forum group. In these discussions, the issue of compensation and support for individuals is one of the top priorities.

Outside of our discussions with legal advisors, this 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 judgement 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.

2.10 The unknown of what and where our data may be used or not, is very stressful and worrying.

We want you to know that your Pensions Committee, plus the Environment Agency Board and Senior Leadership in the organisation are taking this cyber incident very seriously. They are monitoring Capita closely and want to ensure that members are being supported.

It's also important to recognise that this is still a live incident and there is further work required.

2.11 I've heard that it will cost £15-£20 million for Capita to recover from the incident. Does Capita have insurance to cover this cost so that it will not affect our pension?

Capita have the relevant insurance as you would expect for an organisation of their size. Member pensions are protected in statute. The funds held in EAPF are completely separate and will not be affected by any costs to Capita for the breach. The £15-£20m costs estimated to recover from the incident relate solely to Capita and not the EAPF or any other Capita clients.

2.12 There are lots of firms touting for business in relation to claiming compensation regarding this data breach with regard to the effect on anxiety etc. What is the EAPF's view of this?

The Fund is liaising with its Legal advisors on a number of issues as outlined in question 2.9 and 3.12.

2.13 Are you going to move from Capita following this incident

We procure in line with the guidelines set out by Government. This includes a consideration of how any supplier manages personal data. The process is overseen by Defra Commercial, Independent professional advisors and input from the Pensions Committee.

3.0 The Experian service

3.1 What service can I use to monitor the use of my personal data?

To help you monitor your personal information for certain signs of potential identity theft, you've been provided with a unique code for a free 24 month membership through Experian to 'IdentityWorks Global'. This unique voucher code and the steps to register to the service are included in the letter affected members will receive.

3.2 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.

3.3 How does the Experian service work?

This service notifies individuals via e-mail or SMS whenever there are certain changes to their Experian Fraud Report or instantly alerts them when personal information has been found on the web.

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

As well as the Experian service alerting you via email or SMS if your personal information is found on the web, they also have an education centre which helps you consider the most appropriate steps you could take to protect yourself. This vital insight can help you to determine if you're at risk and to help reduce the risk of becoming a victim of fraud in the future.

3.5 What personal information is monitored by the Experian service?

Experian monitors the dark web, to find specified personally identifiable information. For example, your first name, last name, email address, phone number, debit card and credit card number (max of two), driving licence number, passport number, National Insurance number, IBAN (International bank account number).

3.6 What are the approved countries for IdentityWorks (Global)?

These are the current countries that have been approved for this service:

Australia, Austria, Brazil, Canada, Denmark, Finland, France, Germany, Hong Kong, India, Ireland, Italy, Malaysia, Mexico, Netherlands, New Zealand, Norway, Poland, Portugal, Singapore, Spain, South Africa, Sweden, Switzerland, Turkey, United Kingdom, United States, Puerto Rico, Guam and US Virgin Islands.

3.7 How do I register for the Experian service?

Affected members 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 an email address you can use to contact Experian for any questions you have at **globalidworks@experian.com**.

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 'IdentityWorks', you should log into your existing Experian account and visit the Education centre FAQs for guidance on how to add another account and activate your new code.

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 may you hold a credit card with or may have a loan with.

However, in addition it is optional to add specific account details if you'd like these accounts to be monitored 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 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 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 further bespoke information on an Experian alert you've received, there is a dedicated email address to help members who have questions or concerns about this. We'd recommend contacting the Experian team at **globalidworks@experian.com** to see if they can provide more information on the alert you received.

3.11 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: **Phishing: Spot and report scam emails, texts, websites and... - NCSC.GOV.UK**

3.12 Why were we only provided with 12 months Experian monitoring originally? The data can be out there forever for criminals to use.

Capita had advised that 12 months was appropriate for this type of incident.

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

This will take effect automatically, so there's nothing for you to do. If you've already registered with Experian, your membership will lapse 24 months from the date you registered.

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.

The EAPF are continuing discussions with the internal EA legal team and our external legal advisors regarding the data breach, including various aspects of the support Capita have put in place.

3.13 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.

3.14 Why should we have to provide another third party with our personal data to access support?

We appreciate the irony in the need to provide personal information to Experian, however this is necessary for them to be able to accurately monitor the situation for you.

The Experian service provides individuals access to their Experian Fraud Report where alerts and certain changes can be viewed, such as a loan application. Individuals will also be alerted via email of personal information found on the web via their web monitoring service. It

In order to gain access to this Fraud report, it's inevitable that Experian will need your details to be able to monitor the risk for you. It is your choice whether or not you wish to sign up to the Experian service. So, if you don't wish to share your information with another third party supplier then you don't have to.

But Experian are a leading identity protection service who specialise in the protection of data. They provide a trusted facility, which can provide peace of mind that you'll be alerted if you're at threat of becoming a victim of fraud.

3.15 Will this affect those already receiving, or who are about to receive, state pensions?

No it will not. Neither your state pension, nor your EAPF pension, were impacted by the incident. The incident will not affect your upcoming, or already received, pensions.

The impact of the incident is limited to the exfiltration of certain data held by Capita in relation to your EAPF pension, so we are making you aware of the situation and recommending you register with Experian and stay vigilant.

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

Unfortunately, as 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 members 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.

Capita has made it 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 are unable to provide your consent for them to contact Experian on your behalf.

If you have further questions on this, Experian can be contacted by email at **globalidworks@experian.com**. The people there understand the service and how it works.

3.17 Could somebody contact Capita posing as me and change my bank details? (For a pensioner member)

We have confirmed this with Capita and are satisfied that they have robust identity and verification procedures to be assured an individual making contact is indeed a member of the EAPF. Changes to the personal details Capita currently holds about you require additional evidence to be provided to verify any change.

For bank changes – these are not accepted over the phone because of the security risk this poses – and evidence of the change must be provided.

From the assurances and procedures outlined by Capita to us, it is clear that it would be very unlikely that bank details could be changed by anyone other than our members.

3.18 Is there any business link between Capita and Experian?

This is a question that has been asked following our mailings and Capita have confirmed that there is no business link between Capita and Experian.

Experian were chosen from the 3 main providers of identity monitoring, because they were able to offer the most appropriate level of support.

3.19 What if I have other questions not covered here?

We have done our best to cover as many questions as possible. We have also updated these questions on 10 October following further queries raised after the mailing reached our members.

We'd urge you to set up your Experian service and contact them if you have any questions. If you have other questions that you want to ask Capita, please do be patient with the team. The incident has had an impact on their 'business as usual' processing, and they're recovering from lost time as a result of the cyber incident at an already busy time.