The Experian service

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.

2 How does the Experian service work?

This service notifies registered 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 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.

4 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 on **020 8090 3696,** or by 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.

5. I have already paid £25 for a CIFAS protective registration flag. Can I get a refund?

If using the Experian service, you are identified as a victim of fraud, the CIFAS protective registration flag forms part of the service and is free of charge.

However, if you independently choose to pay for this flag without the service identifying you as a victim (or have previously paid for it prior to this incident), the cost to you cannot be refunded.

6. Do I need to give Experian my bank details?

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.

7. What else can Experian do to protect me?

Within your Experian account, 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.

8. What exactly is the third-party monitoring looking for? Why are you telling us there is no signs of the data when I've had an Experian notification saying my details have been found on the web?

Capita have appointed third-party experts who have been monitoring the dark web on a daily basis, looking for evidence of matches to the exfiltrated data. To date, no evidence has been found matching the Capita data that was breached in the attack.

The dark web is a part of the internet that is hidden from public search engines and can only be accessed by using special software. The specialist team who are providing this monitoring, use a tool that can access the dark web. The software they use scans the dark web specifically for matches to the Capita data that was included in the exfiltrated data.

We were aware of newspaper articles in the very early days of the attack, suggesting that some samples of Capita data may have been for sale on the dark web. There were artefacts on the dark web that claimed to be from Capita systems. The third party monitoring as mentioned, has found no evidence that information relating to this incident is, or has been, available for sale online to date. In particular, Capita understands that an apparent online link to purchase the alleged Capita data, which has been reported in some newspapers, has never been activated.

As there remains no evidence of the data being found, in Capita's view any fraudulent activity picked up to date isn't therefore linked to the cyber attack. With the Experian membership in place, they believe members are also now that much more aware of any unusual activity, which can only be a good thing.

The Experian service is completely separate from Capita's third party monitoring. It looks for evidence of the information they have for registered members using the verified information on their profile, and anything additional that individuals choose to be monitored. This may include other email accounts that were not included in the Capita data breach, or financial information that wasn't included too. Some members have reported to us that they have received Experian alerts and have assumed that this is part of the data breach.

Unfortunately, the digital era we live in has seen a significant increase in criminal cyber attacks in recent times. Many of these attacks go unreported to the victims whose data has been breached. We do believe that having the Experian service available is key to increased awareness of when details are found – making it possible for those receiving the alerts to take action when this is the case.

Any alerts through the Experian service will include the data item that has been found on the web, but it will not confirm the date this data first appeared on the web – which could go back up to 6 years prior to registering with the Experian service. Unfortunately, Experian also cannot ascertain the source of any identity information located as a result of its scans and searches

The alert may ask some questions to confirm whether the member recognises it and will give some recommended steps they should take to keep their details safe – such as changing passwords, or contacting them for something of greater concern.

Both Capita and Experian advise that the steps set out are the best way to protect members who receive these alerts.

It's also been a common cause of concern where members have previously used a comparison service for financial services such as insurance. Many of these sites will perform a search automatically in the lead up to the anniversary of the renewal date. Often, this will create multiple notifications on the Experian service – which can cause concern for members who don't recognise that they have applied for anything. However, where this is the case it's often explained by an upcoming renewal for any form of insurance previously taken out.

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

As confirmed in question 8, 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.

The Experian service is there to alert members If there was anything untoward happening to your personal email address online, the activity would be flagged via Experian. But this activity isn't likely to be linked to the Capita data breach as explained above in question 8.

The Experian alert members may receive would include recommendations of steps you can take to keep your information safe - such as changing email account passwords or contacting them for anything of greater concern. And if you have any concerns you can raise these 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**

10. I've noticed an increase in spam texts and phone calls too since the cyber incident, are these linked to the breach?

Phone numbers were not included in the exfiltrated Capita data. Therefore, this cannot be linked to the cyber breach. As explained in question 8 above, there are commonly breaches that go unreported and so any increase in spam texts or calls may be linked to something separate.

11. When will the Experian membership update to show 24 months rather than the initial 12 months that was provided?

When we initially agreed that the membership would be updated to 24 months, we were given incorrect information about how the update would be made to the Experian service. It was indicated that this would be done within 3 months of registering for the service.

Unfortunately, this has taken longer than Experian had anticipated, which means that it's possible that it may still show as a 12 month membership.

Experian have recently confirmed that they have committed to updating all member accounts by their expiry date. **Therefore, your account will show a further 12 month membership by the anniversary date of when you registered.**

12. What will reduce the chances of becoming a victim of fraud?

When you're registered with the Experian service, if your fraud report identifies fraudulent financial activity, they 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.

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

Experian 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.

14. I didn't set up my Experian service and my code has now expired. Can you send me another one?

Capita have informed us that the letters offering complimentary Experian membership were issued over 6 months ago and included a section headed "Activating your free Identity Plus membership". This made it clear to both clients and members to "Ensure that you sign up for the service by XXXXXXXX 2023 (your code expires after this date)".

In addition, the EAPF used various channels to remind members when their codes were approaching their expiry date.

Up to now, replacement codes have been issued on a case-by-case basis for varying reasons.

For a short period of time, Capita will now only be issuing a new code in exceptional circumstances i.e. where the member did not receive the original letter with the code. No codes will be sent for any other reason once they have expired.

15. 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 14 February following further queries raised since the incident was communicated with affected members.

We'd recommend contacting Experian if you have any questions linked with the Experian service. For other questions that you may have, you can contact Capita at **info@eapf.org.uk** or for anything linked to the management of your pension, you can contact the EAPF management team at **EAPF@environment-agency.org.uk**