**Strictly Private & Confidential**

24 May 2023

Dear ,

**Unipart Group Retirement Benefits Scheme – “the Scheme”**

I, John Neill, write in relation to your pension and data held within the Scheme, by the external administrator Capita Pension Solutions Limited (“Capita”). **I regret to inform you that some of your personal data was likely to have been stolen by fraudsters**. Your pension, and the payment of your pension, is not affected by this data breach.

This letter provides very important information to explain:

* What personal data was stolen?
* How was the data stolen?
* How you can protect yourself from fraudsters?
* Additional support available to help protect you.

**If you receive an unexpected telephone call from someone claiming that they are either from Capita, the Scheme or that your pension is at risk, please “hang-up” and end that call immediately - AS IT COULD BE A FRAUDSTER AND SCAM.** Then, either wait 10 minutes (to ensure the telephone line has cleared and the “fraudster” is not still connected) or use another telephone number if you are able, and call the dedicated Experian helpline on 0800 229 4005 (UK) or [020 8629 5979](https://urldefense.com/v3/__https:/manager.ng-in.com/effective/routing.serviceNumbers.form?edit*263723*&CSRF_NONCE=C55621AEDB582931E7BF911017969F0F__;W10!!MfzFaTml5A!jyYkhFJWijXugkon4BViIT7mdtNqaSgfYK-90FtTvskqeFoBmQdPREAs5PLVTyhrDsjcrZPjuDY0yXOdNHfMsjFWmUcAmA$) (if overseas). You may also call the **Unipart member helpline** on 0344 391 2421 if you have a query relating to your benefit.

What personal data was stolen?

The personal data stolen by the fraudsters includes the following:

* Name;
* Member unique identification number;
* National Insurance number;
* Pension paid;
* Tax code;
* Tax paid;
* Other deductions (where applicable)

For some, but not all, of the affected members, in addition to the above the personal data the following data was also stolen:

* Date of birth;
* Date of retirement or date of pension cessation.

How was the data stolen?

Capita is the appointed administrator for the Scheme (as well as hundreds of other pension schemes) and they undertake all the administration tasks including, maintaining the Scheme records on their technology system (“Hartlink”), and calculating and paying the pension benefits due to each Scheme member.

Capita reported on 3 April 2023 that they had been subject to a “cyber attack” where fraudsters targeted and accessed some of Capita’s computer servers – potentially impacting several of the cross-sector businesses it serves. Since then, the Trustee has been liaising closely with Capita to understand whether any of our Scheme data has been impacted. On Thursday 18 May we were informed by Capita that details of some Scheme members were held in data files, on the Capita servers, that had been accessed and stolen by the fraudsters.

We are truly sorry that your data has been accessed and stolen in this way and understand that this news will be very concerning to you. We are proactively engaging with Capita in respect of their ongoing investigations to ensure the security of our member data.

**Please be assured that your pension and payments are unaffected by this attack.**

I can also confirm that the Hartlink system, which holds all your personal data, was not impacted by this attack.

How you can yourself from fraudsters?

We live in a data driven world and unfortunately cyber attacks by fraudsters and scams are a real and increasing risk threat to everyone. We would encourage you to only ever give out personal information if you are absolutely sure you know who you are communicating with.

Please also be particularly vigilant if you receive any unexpected emails, telephone calls, text messages (including WhatsApp), letters or you are approached in person. **Please be careful not to share any personal or financial information in such instances**, and check your bank, building society and credit card accounts regularly for any unusual activity that you do not recognise.

The following is a list of organisations who provide information and support to help protect yourself against hackers and cyber criminals:

* If you receive a suspicious email, you should forward it to Action Fraud at [report@phishing.gov.uk](mailto:report@phishing.gov.uk) or call 0300 123 2040. Further information is available on Action Fraud’s website (www.actionfraud.police.uk).
* 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.
* Enclosed is a copy of the Financial Conduct Authority’s (FCA) ScamSmart leaflet and further information to help protect yourself from scams is available on the FCA’s website (www.fca.org.uk/consumers/pension-scams).
* Consider whether any passwords and/or security questions for website logins may need to be changed.
* If you are concerned someone might be impersonating Capita or the Scheme, please contact Capita in the first instance on 0344 391 2421 or unipart@capita.com.

The [National Cyber Security Centre](https://www.ncsc.gov.uk/guidance/data-breaches) (www.ncsc.gov.uk) and the [Information Commissioner’s Office](https://ico.org.uk/for-the-public/) (www.ico.org.uk) both provide guidance on their websites that you may also find useful.

Additional support available to help protect you

The Trustee recognises that this incident places you at a heightened risk of fraud and scams. To support protecting you from this, Capita has arranged a complimentary 12-month membership to **IdentityWorksSM** provided by Experian, one of the UK’s leading Credit Reference agencies. The **IdentityWorksSM** service monitors the web**,** social networks and public databases on your behalf 24/7, looking for your details to immediately detect theft, loss or disclosure of your vital personal and financial information.

If your information is found, you’ll be instantly alerted and given help and advice on what to do next to protect yourself from fraud.

**Activating your free Experian IdentityWorksSM** **membership**

1. Ensure that you sign up for the service by *24 August 2023* (your code expires after this date).
2. Visit the IdentityWorksSM website to get started: [www.globalidworks.com/identity1](http://www.globalidworks.com/identity1)
3. Click on ‘Get Started’
4. Enter your details along with the following activation code:

Once your membership is activated, you’ll have access to the following features:

* **Internet Surveillance**: Technology searches the web, chat rooms & bulletin boards 24/7 to identify trading or selling of your personal information on the Dark Web.
* **Fraud remediation tips**: Self-help tips are available on your member centre.

If you have any questions regarding this service, you can contact Experian’s Customer Support Centre on 0800 229 4005 (UK) or [020 8629 5979](https://urldefense.com/v3/__https:/manager.ng-in.com/effective/routing.serviceNumbers.form?edit*263723*&CSRF_NONCE=C55621AEDB582931E7BF911017969F0F__;W10!!MfzFaTml5A!jyYkhFJWijXugkon4BViIT7mdtNqaSgfYK-90FtTvskqeFoBmQdPREAs5PLVTyhrDsjcrZPjuDY0yXOdNHfMsjFWmUcAmA$) (if overseas). The Support Centre is open Monday to Friday, 8am to 6pm.

Reporting the incident to Regulatory bodies

We have reported this incident to the [Information Commissioner’s Office](https://ico.org.uk/for-the-public/) and will work with them on any investigation they choose to conduct and any recommendations they might subsequently make. We have also informed the Pensions Regulator and we are aware that Capita have been in close contact with both these regulatory bodies since identifying that an incident had taken place.

What happens next?

We will continue to work closely with Capita to understand which members were affected by the data breach. As soon as we have received confirmation, we will write to the affected members to let them know that their data was exfiltrated.

Even if your data was ultimately not exfiltrated, the Trustees would recommend that you sign up for the Experian Identity Plus.

A generic copy of the letter and FAQs enclosed will be published on the Trustee website (<https://www.unipartpensions.com/>).

Once again we are truly sorry for any distress and inconvenience that this attack may cause you, and please exercise extra caution if you receive any requests to provide or confirm your personal data. If you have any questions relating to this attack you can contact the member helpline on 0344 391 2421.

Yours sincerely



**J M Neill**

**Chair of UGC Retirement Benefits Trustees Limited**

**Trustee to the Scheme**

| **Question** | **Answer** |
| --- | --- |
| What happened? | Capita plc recently reported a cyber incident (<https://www.capita.com/news/update-actions-taken-resolve-cyber-incident>) involving hackers targeting some of its computer servers. Some of these servers were used by Capita Pensions Solutions, which is a business that provides third party pension administration to several pension schemes in the UK, including Unipart Group Retirement Benefits Scheme  As part of this breach, Capita have confirmed that some of our Scheme data was exfiltrated. |
| When did it happen? | Capita detected the cyber incident on 31 March 2023 and took immediate steps to isolate and contain the issue. Since then, it has undertaken a complex forensic investigation with support from technical experts and specialist advisers. This has involved reviewing files across Capita’s entire business. |
| What does exfiltrated mean? | It means that the data file was accessed and/or copied by the hackers. |
| What is being done about this? | The Trustees are in close contact with Capita and we are proactively engaging with them in respect of their ongoing investigations.  We are also engaging with Capita regarding the ongoing support they are providing for those affected. |
| Was the Hartlink system compromised? | Capita have stated it was only a server affected and data held on Hartlink cloud based computing (such as log on details) were not exfiltrated. |
| Is this going to impact my pension payments? | Please rest assured that your pension payments are unaffected by this and will continue as normal. |
| What about my pension benefits? | The hackers only accessed data. The Scheme’s assets were not involved and are held completely separately from Capita. |
| Are all members affected? | No.  This has affected the majority of pensioner members, including dependent pensioner members. As far as we are aware deferred members are not affected. |
| What happens next? | We will continue to work closely with Capita and we will be in contact shortly to confirm whether your data was part of the breach.  We will continue to communicate all relevant information to you as soon as we are aware of it.  A generic copy of the letter as well as a copy of this FAQ will be published on the Trustee website (<https://www.unipartpensions.com/>). |
| What can I do to protect myself? | Please ensure that you use the Experian service provided. Further details and your unique Experian code are available in the letter enclosed.  We have also included a leaflet in the letters from the FCA on Pensions Scams.  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](mailto:report@phishing.gov.uk).  For text messages and telephone calls, forward the information to 7726 (free of charge), which reports them to Ofcom.  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. They will never email you.  The [National Cyber Security Centre (https://www.ncsc.gov.uk/guidance/data-breaches)](file:///\\srv468\pensions\Capita\Cyber%20Incident%20-%20March_April%202023\National%20Cyber%20Security%20Centre%20%20(https:\www.ncsc.gov.uk\guidance\data-breaches)) and the Information Commissioner’s Office (https://ico.org.uk/for-the-public/) (ICO) both provide guidance that may also be useful. |
| Have you informed the Information Commissioner’s Office (ICO)? | Yes |
| Have you informed Unipart? | Yes. |
| Have you informed The Pensions Regulator? | Yes. |
| What are the Trustees doing to make sure this doesn’t happen again? | In our discussions with Capita, we have sought information about what it has done to improve the security of personal data and avoid a future incident. Once the investigation has been finalised, we will receive 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. |
| I have questions not answered here. | If you have a query relating to the Capita Cyber Incident, please call the dedicated Experian helpline on 0800 229 4005 (UK) or [020 8629 5979](https://urldefense.com/v3/__https:/manager.ng-in.com/effective/routing.serviceNumbers.form?edit*263723*&CSRF_NONCE=C55621AEDB582931E7BF911017969F0F__;W10!!MfzFaTml5A!jyYkhFJWijXugkon4BViIT7mdtNqaSgfYK-90FtTvskqeFoBmQdPREAs5PLVTyhrDsjcrZPjuDY0yXOdNHfMsjFWmUcAmA$) (if overseas).  You may also call the **Unipart member helpline** on 0344 391 2421 if you have a query relating to your benefit. |



