

Fraud Guidance

This document has been prepared in our capacity as third party administrators to a variety of UK based pension Schemes (Third Party Administrators). It's intended to provide some high level guidance and information about the types of fraudulent activity that can commonly be experienced by pension scheme members, savers and investors.

Fraud is ever evolving, and this document isn't intended to provide an exhaustive list of the types of fraudulent activity that can be experienced or all of the steps that you might want to take to protect yourself. For further detailed guidance and information, you should refer to the links contained in this document.

Background

Modern technology offers criminals an opportunity to approach pension scheme members, savers and investors (especially the more vulnerable in our society) who may be worried about their finances.

Fraud is the deliberate use of deception or dishonesty to deprive, disadvantage or cause loss (usually financial) to another person or party. Often criminals will pose as a genuine firm, pretending to offer you help and guidance.

They may use fraudulent emails, phone calls, text messages or social media posts claiming to provide security for your money, offering new and exciting investment opportunities or advertising 'early access' pension offers.

Scams are hard to spot and are often disguised with believable websites, testimonials and materials which make them look like the real thing. If you don't spot these as fraudulent activities, you could end up disclosing personal or financial information or clicking on links within emails or text messages that may contain viruses or lead to fake websites allowing the criminal to misuse your data for fraudulent purposes. Pension scammers are targeting honest people like you with the average victim losing as much as £91,000.

(Source: The Pensions Regulator, www.thepensionsregulator.gov.uk)

Don't let a scammer enjoy your retirement.

How to protect yourself

Top 5 Things to look out for:

- Unsolicited requests to disclose personal details (such as name, address, bank details, email or phone number) – remember, financial institutions will not ask you to click on a link to confirm your bank or personal details.
- 'too good to be true' offers using words like 'savings advance', 'cash incentive', 'bonus', 'loophole', 'one-off investment opportunities', 'free pension reviews', 'government endorsement', 'overseas investment'.

- Advice that you can access your pension before age 55.
- Emails not from Hymans Robertson asking you to click on a link to Prism (our emails will always end with @hymans.co.uk).
- Pressure to transfer funds or to make a quick decision.

If something doesn't feel right or feels too good to be true, trust your gut feeling - take no action.

Advice from the Regulators

To help you spot the signs and protect yourself from a scam, the Financial Conduct Authority (FCA) and The Pensions Regulator suggest the following four simple steps:

Step 1 - Reject unexpected offers - If you're contacted out of the blue about a pension opportunity or a free pension review, chances are it's a scam. Pension cold calling is illegal, and you should be very wary.

Step 2 - Check who you're dealing with - Check the FCA's website (<https://register.fca.org.uk/s/>) to ensure anyone offering you advice is authorised. If they are not, you may not have access to compensation schemes.

Step 3 - Don't be rushed or pressured - Take your time to make all the checks you need – even if this means turning down what seems to be an 'amazing' deal.

Step 4 - Get impartial information or advice - Consider seeking independent financial advice (as per Step 2 above) before changing your pension arrangements. In some cases, e.g. transferring more than £30,000 from a final salary scheme, advice from a registered adviser must be obtained.

If you think you have been a victim of a scam, report it to Action Fraud on 0300 123 2040 or via their website www.actionfraud.police.uk.

You can report an unauthorised firm or a scam to the Financial Conduct Authority by calling them on 0800 111 6768 or by using their online reporting form found at www.fca.org.uk/consumers/report-scam-us.

Useful Websites

You will find a list of common fraud techniques on our website -

<https://www.hymans.co.uk/insights/blogs/blog/be-aware-of-the-approaches-fraudsters-can-take/>

Visit the Government backed MoneyHelper website at <https://www.moneyhelper.org.uk/en/pensions-and-retirement?source=tpas> for free independent and impartial pensions information and guidance before making any decisions about your retirement savings.

Be ScamSmart with your pension. To find out more, visit www.fca.org.uk/scamsmart

Hymans Robertson Pension Scheme Administration Teams

Fraud Guidance (Appendices)

Definitions

<p>Phishing</p>	<p>Phishing is a method used by fraudsters to access valuable personal details, such as usernames and passwords.</p> <p>These can have a monetary value to criminals. Phishing can also involve sending malicious attachments or website links in an effort to infect computers or mobile devices. Criminals send bogus communications: emails, letters, instant messages or text messages. Very often these appear to be authentic communications from legitimate organisations. Embedded links within the message can direct you to a hoax website where your login or personal details may be requested. You may also run the risk of your computer or smartphone being infected by viruses.</p> <p>Once your personal details have been accessed, criminals can then record this information and use it to commit fraud crimes such as identity theft and bank fraud.</p> <p>Phishing messages generally try to convince the recipient that they are from a trusted source. “Spear-phishing” is a technique whereby criminals use personal information to earn trust and lower the intended victim’s defences increasing the chances they may open attachments or embedded links.</p> <p>Criminals have stepped up their activity by targeting business users by claiming that they have specific knowledge of the business. These may be business critical issues: customer feedback, requests for information, staffing or legal notices.</p> <p>(Source: Action Fraud)</p>
<p>Smishing</p>	<p>Smishing is when criminals use text messages impersonating other organisations to trick people into giving away their personal and financial information or money. These scam texts often claim to be from government departments, banks or other trusted organisations, offering payments related to the coronavirus outbreak or claiming to be issuing fines.</p> <p>Often the messages will include a link to a fake website that is designed to trick people into giving away their financial and personal information such as bank details, passwords and credit card numbers. Criminals are also using a technique called “spoofing”, which can make a message appear in a chain of texts alongside previous genuine messages from that organisation. The banking industry continues to work closely with mobile network operators, government, and other industry stakeholders to crack down on this type of fraud.</p> <p>(Source: UK finance)</p>

Vishing	<p>The word 'vishing' is a combination of 'voice' and 'phishing.' Phishing is the practice of using deception to get you to reveal personal, sensitive, or confidential information. However, instead of using email, regular phone calls, or fake websites like phishers do, vishers use an internet telephone service (VoIP).</p> <p>Impersonating a person or legitimate business to scam people isn't a new thing. Vishing is simply a new twist on an old routine. In fact, vishing has been around almost as long as internet phone service.</p> <p>Using a combination of scare tactics and emotional manipulation, they try to trick people into giving up their information. These vishers even create fake Caller ID profiles (called 'Caller ID spoofing') which make the phone numbers seem legitimate. The goal of vishing is simple: steal your money, your identity, or both.</p> <p>(Source: Fraudwatchinternational)</p>
----------------	---

Specific Guidance

Phishing guidance:

- check that the sender email address looks correct
- look for spelling mistakes in the email
- if there is a hyperlink within the email text be suspicious
- be wary of generic salutations (e.g. Dear colleague instead of Dear Gillian) or the lack of a salutation
- don't feel pressured by threats within the email e.g. "If you do not respond, your pension benefits will be frozen"
- ignore requests to take immediate action/urgency.

Further guidance can be found at www.actionfraud.police.uk/a-z-of-fraud/phishing.

Smishing guidance:

As above for phishing but in relation to text messages however, more specifically

- do not click on a link contained within a text
- if the text is unprompted then be wary
- ask yourself if you usually receive texts from the sender of the text, if not be suspicious.

Vishing guidance:

- Be aware of unsolicited calls
- Do not share any personal details when receiving an unsolicited call
- Be wary of promises of high returns, the offer of a free pensions review, advising you can access your pension before age 55
- Don't feel pressured into making a decision or taking any action.

Further guidance can be found at www.fca.org.uk/scamsmart or www.thepensionsregulator.gov.uk/en/pension-scams.

Examples

Phishing emails:

From: Michael Steinitz <michaelst@ekmd.huji.ac.il>
Date: 27 March 2020 at 14:51:10 GMT
To: Michael Steinitz <michaelst@ekmd.huji.ac.il>
Subject: March & April payment benefit | Covid-19 Update

During these exceptional circumstances, we would like to request the cooperation of everyone to maintain our health and safety in and outside the Institution. Please due to the latest update, all staff & Employee are expected to kindly Click [PRMA](#) and complete the required directive to be added to March and April benefit payroll directory system.

You will be omitted if you fail to comply with the directives.

Thank you,
 Admin Department .

Phishing emails:

HMRC is aware of a phishing campaign telling customers they can claim a tax refund to help protect themselves from the coronavirus outbreak.

Do not reply to the email and do not open any links in the message.

The email has been issued in various formats. An example of this scam is below:

----- Forwarded message -----
From: GOV UK Notify <danielhhs@pinkcontract.com>
To: *
Sent: Friday, 6 March 2020, 08:28:50 GMT
Subject: UK Updates on COVID-19

The government has taken urgent steps to list coronavirus as a notifiable disease in law

As a precaution measure against COVID-19 in cooperation with National Insurance and National Health Services the government established new tax refund programme for dealing with the coronavirus outbreak in its action plan.

You are eligible to get a *tax refund (rebate)* of 128.34 GBP.

[Access your funds now](#)

[The funds can be used to protect yourself against COVID-19(<https://www.nhs.uk/conditions/coronavirus-covid-19/> precautionary measure against corona)

At 6.15pm on 5 March 2020, a statutory instrument was made into law that adds COVID-19 to the list of notifiable diseases and SARS-COV-2 to the list of notifiable causative agents.

From Government Gateway

This is an automatic email - please don't reply.

Fake letters:

HM Government

This is a nationwide appeal in support of our efforts against Coronavirus (COVID-19)

The NHS associates are looking for individuals who can support in the purchase of medical preparations and supplies for mental health support and other initiatives to support staff and more - not just now, but in the weeks and months to come.

This is part of the Government's response to Coronavirus (COVID-19).

During this time of crisis, the NHS staff provide care for you and your family. Now it's our time to support all the NHS staff provide care for you and your family. Now it's our time to support all the NHS staff provide care for you and your family. Now it's our time to support all the NHS staff provide care for you and your family. Now it's our time to support all the NHS staff provide care for you and your family.

Right now, our staff are under an unprecedented amount of pressure and are working around the clock to deal with the impact of COVID-19. They are literally pulling out all the stops to ensure they are providing the very best of care now - and that they will be able to cope with the predicted daily pressures of the virus.

Let's help them. We can all do this. It is a crucial fight. Please make a donation to support our country. For the NHS staff who are fighting the virus and for the NHS staff who are fighting the virus. For the NHS staff who are fighting the virus and for the NHS staff who are fighting the virus.

Monthly financial reports will be provided to all of our supporters in order to track the expenditures of every penny earned in the fight against COVID-19. It will be available at the NHS England website at the end of each month.

Please do not hesitate to make a donation to support our NHS staff who are fighting the virus. For the NHS staff who are fighting the virus and for the NHS staff who are fighting the virus.

Stay at home. Avoid the shops, clubs and work (but only if you cannot work from home).

- * Only go outside for food, medicine or work (but only if you cannot work from home).
- * Stay 2 metres (6ft) away from other people
- * Wash your hands as soon as you get home

Donations made via bank transfer:

Fake texts:

'Goodwill payment' SMS

HMRC is aware of coronavirus SMS scams telling customers they can claim a 'goodwill payment'. Do not reply to the SMS and do not open any links in the message.

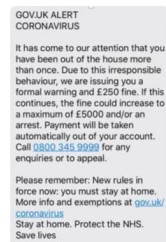
This is an example of the scam wording:

'As Part of the NHS promise to battle the COV-19virus, HMRC has issued a payment of £258 as a goodwill payment. Follow link to apply.'

'£250 fine' SMS

HMRC is aware of a SMS scam which states you will be fined £250 for leaving the house more than once. The message asks recipients to call an 0800 telephone number to appeal.

Do not reply to the SMS or call the phone number listed. An example of the scam is shown below:



City of London Police hasn't issued any alerts about fake messages from Danske Bank.



We are aware of a rumour currently circulating via WhatsApp, SMS and social media which references the City of London Police Fraud Team and claims that Danske Bank customers are being targeted by a particular text message (smishing) scam. The contents of this message is false.

Additional Guidance

You can obtain further information from the following agency websites on the different tactics fraudsters can take and how to protect yourself from such approaches:

Action Fraud, www.actionfraud.police.uk/a-z-of-fraud/pension-scams

Action Fraud, www.actionfraud.police.uk/individual-protection

The Pensions Regulator (TPR) leaflet, www.thepensionsregulator.gov.uk/-/media/thepensionsregulator/files/import/pdf/16423_pensions_consumer_leaflet_screen.ashx

The Money Helper website, <https://www.moneyhelper.org.uk/en>

Hymans Robertson Pension Scheme Administration Teams