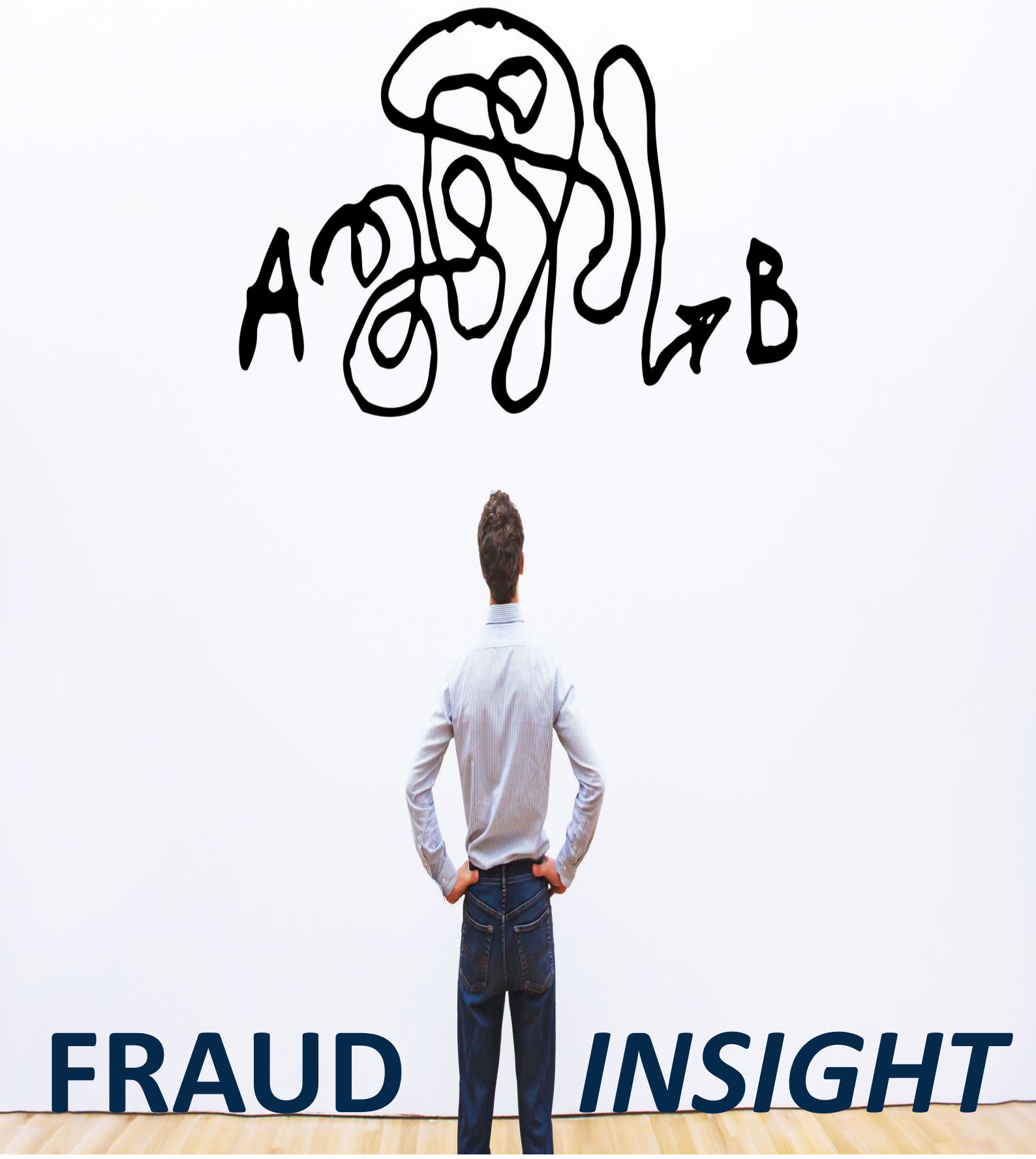

FRAUD INSIGHT

JULY 2022

auditone
assurance . counter fraud . advisory

DOES THE NHS REALLY HAVE A PROBLEM WITH FRAUD AND BRIBERY?

Yes it does. It is estimated that the NHS loses £1.21 billion per year, or roughly £3.3 million per day, to fraud. This is taxpayers' money that is taken away from patient care and falls into the hands of criminals. This is enough money to pay for over 40,000 staff nurses, or to purchase over 5,000 emergency ambulances. When we say 'fraud', we refer to a range of economic crimes, such as fraud, bribery and corruption or any other illegal acts committed by an individual or group of individuals to obtain a financial or professional gain. AuditOne, is a specialist counter fraud provider who works closely with your organisation to combat fraud. We have a team of experienced counter fraud specialists delivering a full range of counter fraud, bribery and corruption services including prevention, detection and investigation. Our professionally qualified counter fraud specialists work to identify potential fraud, bribery and corruption risks through policy and system reviews and suggest remedial action to reduce and mitigate these risks. We are also experienced in carrying out timely criminal investigations, from referral to prosecution. AuditOne is an NHS consortium providing counter fraud services to almost every NHS organisation in the North East and also independent health care providers. It is hosted by Cumbria, Northumberland, Tyne and Wear NHS Foundation Trust and is a not-for-profit organisation.

auditone
assurance . counter fraud . advisory

NHS
Counter Fraud Authority

Our quarterly newsletter highlights real life cases of fraud and bribery that have had an impact on the NHS but also include details of identified scams that could affect you and your families. We include steps that you can take to make sure you do not end up a victim of fraud.

COMMON TYPES OF NHS FRAUD

STAFF

Working elsewhere whilst reported sick. Submitting altered or falsified timesheets. Making false expenses claims including inflated mileage claims. Carrying out private clinical practice in NHS core hours. Carrying out private administrative work for clinicians (drafting notes/letters) in core NHS hours. Providing false information on job applications. Providing false references as part of a job application. Theft and fraudulent use of prescriptions. Diverting NHS money to private bank accounts. Failure to declare criminal convictions.

PATIENTS

False patient travel scheme claims. Providing false personal details to obtain free NHS treatment they are not entitled to. Health Tourists. Multiple registrations in order to obtain medication. Theft and fraudulent use of prescriptions. False lost property claims. False personal injury claims. Obtaining medication/equipment not needed in order to sell on.

SUPPLIERS

Invoicing for goods not supplied. Invoicing for services not provided. Submitting higher value invoices than agreed. Mis-selling of advertising space. Providing lower specification items than agreed. Offering bribes to secure contracts. Supplier collusion to fix tenders.

LOCAL CASE: BISHOP AUCKLAND COUNCILLOR JAILED FOR NHS FRAUD

A Bishop Auckland councillor was handed a 28-month sentence after a trial at Durham Crown Court. The woman, a former Unison representative and County Durham councillor who was elected to Bishop Auckland Town Council in September 2021, was convicted of seven counts of fraud. The court heard how she defrauded both organisations over a four-year period by claiming the same expenses from both organisations. The 58-year-old went on to spend the money on a car, restaurant bills, hotel stays, beauty treatments and even used it to pay for her honeymoon. An investigation uncovered that as Unison's Durham branch secretary and treasurer, had claimed identical expenses from both organisations and often forged signatures of colleagues on cheques to herself to make them look plausible. Two of the offences were committed as an employee of the North of England Commissioning Support Unit (NECS) of the NHS, and six as an official of Unison's Northern Regional Health Commissioning Branch. When she was questioned by Unison she claimed a box containing all her receipts and vouchers had gone missing from a cupboard at her office.

Fraud Investigator, Detective Constable Ali Blackett, of Durham Constabulary's Economic Crime Unit said: "Fraud is a despicable crime that can have far-reaching consequences for victims especially for vital organisation such as the NHS. " (she) not only abused her position of trust in both organisations but went to great lengths to hide her deceit so it is satisfying to see justice served."

UPDATED SCAM ALERT: WHATSAPP FAMILY MEMBER SCAM

New data from Action Fraud, the national reporting centre for fraud and cyber crime, reveals the continued threat posed by a scam that involves criminals contacting victims on WhatsApp and pretending to be their friend or a family member. The scam has been reported to Action Fraud 1,235 times between 3 February and 21 June this year, and has cost users a total of £1.5m. Criminals will typically claim to be a family member and will usually begin the conversation with "Hello Mum" or "Hello Dad". They will say that they are texting from a new mobile number as their phone was lost or damaged and will go on to ask for money to purchase a new phone, or claim that they need money urgently to pay a bill. The criminal will supply their bank details for payment, with some coming back with further demands for money. Criminals are successful in their approach as they are exploiting the emotional vulnerability of the public in an attempt to deceive victims.

How to protect yourself:

- STOP. THINK. CALL. If a family member or friend makes an unusual request on WhatsApp, always call the person to confirm their identity.
- You can report spam messages or block a sender within WhatsApp. Press and hold on the message bubble, select 'Report' and then follow the instructions.
- Never share your account's activation code (that's the 6 digit code you receive via SMS)

Action Fraud advises that the public follow the advice of the Take Five to Stop Fraud campaign to keep themselves safe from fraud.

- **Stop:** Taking a moment to stop and think before parting with your money or information could keep you safe.
- **Challenge:** Could it be fake? It's okay to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- **Protect:** If you think you've been a victim of fraud, contact your bank immediately and report it to Action Fraud online at actionfraud.police.uk or by calling 0300 123 2040.

NATIONAL CASES: GENERAL PRACTICE

CASE 1 - GP struck off after stealing £1.1m from NHS to fund gambling addiction

A senior GP who stole more than £1 million of NHS money to fund his 'desperate' addiction to online gambling has been struck off. The GP embezzled £1.13 million from a healthcare group as he chased the dream of hitting the jackpot on internet slot machines and roulette. The family doctor defrauded the group of GP surgeries immediately after being put in charge of its accounts, leaving its finances in disarray and other directors needing therapy. He was jailed for three years and four months for the fraud by abuse of position in November 2021. In finding the doctor's fitness to practice impaired, the Medical Practitioners Tribunal Chair told him he "placed patients at risk of harm and breached a fundamental tenet of the profession by taking funds that were necessary for patient care."

Case 2 - GP practice manager sentenced for £35,000 pay and pension fraud

A 63-year-old former NHS Practice Manager received 6 month suspended prison sentence for defrauding a GP practice and the NHS Pension Authority of over £35k over an 18-month period, thus gaining in excess of £35,000 in remuneration and pension that she was not entitled to. She had worked as a Practice Manager for over 25 years, commencing in 1997. She was initially employed as a Practice Manager in Pontardawe, before being employed on a part-time basis as the Operations Manager by the Amman Tawe Partnership in 2014. During a meeting that was held on the 24th September 2018, she informed the surgery's partners that the Castle Surgery Practice, Neath, had insufficient funds to pay the staff wages in October 2018. Due to the unprecedented circumstances, the matter was reported to NHS Counter Fraud Officers. As a result of the fraud investigation, it was established that during the period 1st April 2016 to 27th October 2018, she made unauthorised overtime claims totalling £18,506.30 (around twenty-to-thirty hours per month). The subject manipulated and circumvented financial data she had entered into the Practice's GP payroll system, by amending her wages and dishonestly adding the overtime figures, which she also made pensionable. At no point did she seek authorisation for the alleged overtime she worked, whether by the claim procedure or otherwise, in accordance with the Practices' Overtime Policy. She had also increased her salary on a monthly basis starting in April 2016.

NATIONAL CASE: HULL WOMAN GIVEN SUSPENDED JAIL TERM RE NEGLIGENCE CLAIM

A woman who launched a £7.3m medical negligence claim has been given a suspended jail sentence after it was found she made "false statements". The claim, which was made on behalf of her daughter revolved around her daughter's use of a wheelchair. The Court found that she had not told the truth and had exaggerated the claim, with videos showing her daughter dancing in stage shows. The court heard the 38 year old had begun legal action against Hull University Teaching Hospitals NHS Trust before her daughter turned 18 arguing that she had been left disabled because of failings by doctors after she was born with displaced hips. Trust bosses admitted a breach of duty but valued the claim at about £65,000, the court heard. The trust produced footage showing the accused's daughter Megan dancing in stage shows and the claim was reduced from £7.3m to £5.4m. The claimant's daughter subsequently discontinued the litigation after turning 18. The accused was given a six-month jail term suspended for two years.

Spot the signs of holiday fraud

As travel restrictions become more relaxed, Action Fraud, the national reporting centre for fraud and cybercrime, is warning the public to remain vigilant against holiday fraud when booking flights or accommodation online. In the financial year 2021/22, Action Fraud received 4,244 reports of holiday and travel related fraud, a substantial increase of over 120% when compared to the previous financial year. Victims reported losing a total of £7,388,353, an average loss of £1,868 per victim.

Tops tip to avoid falling victim to holiday fraud

- **Stay safe online:** check the web address is legitimate and has not been altered by slight changes to a domain name, such as going from .co.uk to .org.

- **Do your research:** don't just rely on one review, do a thorough online search to ensure the company is credible. If a company is defrauding people, there is a good chance that consumers will post details of their experience, and warnings about the company.

- **Look for the logo:** check whether the company is an ABTA Member. Look for the ABTA logo on the company's website. If you have any doubts, you can verify membership of ABTA online on their website. If you're booking a flight as part of a package holiday and want more information about ATOL protection, or would like to check whether a company is an ATOL holder, visit the CAA website.

- **Pay safe:** wherever possible, pay by credit card. You should avoid paying directly into a private individual's bank account.

- **Check the paperwork:** you should study receipts, invoices and terms and conditions, and be very wary of any companies that don't provide any at all. When booking through a Holiday Club or Timeshare, get the contract thoroughly vetted by a solicitor before signing up.

- **Use your instincts:** if a deal sounds too good to be true, **it probably is.**

For a full list of tips to avoid becoming a victim of fraud, please visit https://www.abta.com/tips-and-advice/planning-and-booking-a-holiday/how-avoid-travel-related-fraud.

FRAUD SPOTLIGHT

The fraud spotlight section of the newsletter focusses on fraud types that commonly occur in the NHS. It provides you with details of how the offences are committed and real life examples of where people have been prosecuted for these offences. This addition looks at:

WORKING WHILST SICK

The problem:

Working elsewhere whilst reported sick continues to be a significant fraud risk for NHS organisations across the country and is now one of the most common offences investigated by NHS counter fraud teams. The ease at which NHS staff can carry out ad hoc temporary work with other NHS organisations through bank and agencies makes the NHS particularly vulnerable to this type of fraud.

How is this offence committed:

It is as simple as it sounds. Staff report sick stating they are unfit to perform their duties either by way of self certification or doctors fit note and then during this period of sickness, carry out any form of paid or voluntary employment or study.

What should I do if I am planning to work for another organisation or study whilst reported sick:

Check your organisations policy on secondary employment and working during periods of sickness. The AuditOne counter fraud team is working with your organisation to make sure the guidance is clear on this but if you are in any doubt you should speak to your line manager before you carry out any employment either paid or voluntary or carry out study whilst reported sick from your NHS employer.

Why is this a criminal matter and not just a disciplinary issue:

NHS employees are in the main entitled to salary sick pay. When reporting sick the employee is declaring they are unfit to perform the required duties of their role and as such are paid for the period of sickness. However if the employee is proven to have misled the organisation about their ability to perform their role, they are unlikely to have been entitled to that sick pay. They have therefore deliberately caused a financial loss to the organisation and been dishonest in their actions.

CASE STUDY 1:

A member of staff who worked within the hospitals telephony service reported sick for a period of three months stating she had injured her back which meant she could not get out of bed and was therefore unfit to attend work. The employee was offered support by the hospital throughout her sickness period and alterations made to her working environment to assist her when she returned. However during her period of sickness the employee emailed her line manager from an email account linked to a private hospital ten miles from the NHS hospital where they worked. Concerns were raised about the legitimacy of the sickness period and a criminal investigation was led by the counter fraud team. The investigation revealed that the employee had deliberately reported sick with the NHS in order to carry out temporary work with the private hospital. She started work with the private hospital on the first day of her period of sickness. The employee received a suspended prison sentence, was dismissed by both organisations and had to repay all of the money she had fraudulently obtained.

CASE STUDY 2:

A specialist dentist employed by an NHS hospital reported sick for a fourteen month period stating treatment she had received for cancer meant she suffered intermittent issues with loss of feelings in her hands therefore couldn't carry out surgery which was a key part of her role. The Trust supported the dentist throughout paying her in excess of £71k during her sickness period. An allegation was received that the dentist was working elsewhere and an investigation revealed that the dentist had been working at four separate dental practices for the entire period of sickness. On one occasion she attended a sickness management meeting in the morning where she maintained she had no feelings in her hands only to drive 100 miles from the hospital where she treated 20 patients in the afternoon. The dentist faced prosecution, was dismissed by the NHS Hospital and was forced to repay the £71k she had stolen.

SCAM ALERT: A TICKET TO NOWHERE

New data from Action Fraud, the national reporting centre for fraud and cybercrime, reveals that 4,982 people fell victim to ticket fraud in the 2021/22 financial year. Action Fraud received 623 reports of ticket fraud in September last year, the highest number of reports received since March 2020, as most festivals and events operated as usual for the first time since pre-pandemic.

Detective Chief Inspector Craig Mullish, from the City of London Police, said: “Criminals took advantage of coronavirus restrictions being lifted last summer and targeted victims looking for tickets to high-profile sporting events and festivals. We have seen reports of ticket fraud rise further this year as well. Many festivals and events for the summer have already sold out, so don’t be deceived by offers on secondary ticketing websites or social media, as this is often where criminals will advertise fake tickets to popular and sold out events. Remember: if a deal sounds too good to be true, it probably is.”

During the 2021/22 financial year, victims reported losing £3.8 million to ticket fraud – an average loss of over £750 per victim. The highest percentage of reports (27 per cent) came from 20 to 29 year-olds and almost half (48 per cent) of victims were aged 20 to 49 years old.

Spot the signs of ticket fraud and protect yourself:

- Only buy tickets from the venue’s box office, official promoter or agent, or a well-known and reputable ticket site.
- Avoid paying for tickets by bank transfer, especially if buying from someone unknown. Credit card or payment services such as PayPal give you a better chance of recovering your money if you become a victim of fraud.
- Be wary of unsolicited emails, texts or adverts offering unbelievably good deals on tickets. If it sounds too good to be true, it probably is.
- Is the vendor a member of STAR? If they are, the company has signed up to their strict governing standards. STAR also offers an approved Alternative Dispute Resolution service to help customers with outstanding complaints. For more information: star.org.uk/buy_safe

---

SCAM ALERT: FAKE CELEBRITY TESTIMONIALS

TV presenter Holly Willoughby is among a growing number of celebrities whose images and fake recommendations are being used in Facebook ads claiming to have made a huge return on a £200 cryptocurrency investment.

In one instance, the scammer convinced one victim to keep sending them money over a number of months, taking £370,000 from them in total. Other celebrities who whose images are being used alongside fake testimonials included Piers Morgan, Sir Richard Branson, Elon Musk and Bill Gates. The face of money saving expert Martin Lewis was also used to con people out of cash, with one victim losing £317,000 after believing he was promoting a "Bitcoin evolution".

Always remember to take 5 when considering parting with you money. STOP just take five mins to consider it, CHALLENGE could this be fake and PROTECT tell your bank immediately if you think you have been scammed.

MoneySavingExpert

Cutting your costs, fighting your corner

Founder, Martin Lewis · Editor-in-Chief, Marcus Herbert

Criminals are increasingly trying to capitalise on the cost of living crisis by targeting households with bogus offers of rebates, grants and support payments. But official Government support payments are usually automatic, so if you get a request for information out of the blue via text, email, or phone call – be wary.

Texts asking you to claim or apply for cost of living help

You DON'T need to apply or do anything else to claim the cost of living payment, which is initially worth £326. If you're eligible, you'll automatically receive the money straight into your bank account. The Department for Work and Pensions (DWP) has said that it had seen texts claiming to come from "Gov.org" and one which said it was from DWP. It added that some people had received scam texts followed up by an email asking them to call a fake number to provide more info. So if you see texts or emails asking you to provide details to claim for the help be wary and report them.

Messages from 'Councils' asking for bank details for £150 tax rebate

Councils across the nation have urged households not to give out their bank or card details over the phone if they get a call about the £150 council tax rebate. The MSE website said: "In most cases, the rebate is paid automatically to those who pay their council tax by direct debit - and most people who pay by direct debit should have received their payment by now. For those who don't pay by direct debit, most councils are collecting bank details using secure online forms. If you get a call and you're not sure the caller is genuine, hang up and call your council directly using the contact number on its website.

Messages claiming that Ofgem is offering a £400 energy rebate

Ofgem is NOT offering a £400 energy rebate - so beware scammers telling you this.

Further information about these scams and other really helpful advice and guidance can be found on the money saving expert website:

https://www.moneysavingexpert.com/news/2022/07/dwp-cost-of-living-scam-texts-warning/

PRESENTATIONS: CAN YOU HELP?

As your fraud provider we are always looking at ways to raise the profile of the counter fraud team within your organisation. One of the key ways we do this is by delivering counter fraud presentations. Our interactive presentation focuses on real life fraud cases with mainly news clippings and the stories behind them. We tie this in with the use of digital clickers which each attendee is given at the start of the presentation and is asked to vote/answer questions throughout (who wants to be a millionaire style). The presentation can be tailored to suit the audience and time available. So if you have a monthly/quarterly team meeting and fancy hearing from a team you might not ordinarily consider why not give us a go. Contact details for the team can be found on the last page of this newsletter or by searching fraud on your organisations intranet.

SCAM ALERT: CALLOUS PENSION FRAUDSTERS JAILED FOLLOWING £13M SCAM

Two fraudsters have been jailed for their part in a series of scams in which 245 people lost millions of pounds in pension savings. The man, 62, and women, 66, tricked people into transferring savings to schemes supposedly investing in property or "truffle trees". Unsuspecting victims transferred more than £13m of pension savings which were used by the fraudsters to live a life of luxury including skiing holidays and trips to Dubai.

The man was jailed for five years and seven months while the woman was jailed for four years and eight months. Both stood and looked straight ahead in the dock as the sentences were handed down. Passing sentence, Judge Gregory Perrins said the pair caused "such misery to so many people", with victims suffering mental health problems and some even attempting suicide. Each account that I have read is a story of a life ruined by your actions and you should both be ashamed," he said. In heart-breaking testimony, one 62 year old victim who thought he was investing in overseas property and lost over £100k said "'I have nothing. My pension has gone. I am going to have to work for the rest of my life".

The accused ran 10 dishonest pension schemes and were ordered to pay a combined £13.6 million to those who had lost out. However, none of the victims have yet to receive a penny of the money they should have been refunded. In addition to their jail terms, both have been banned from being directors of companies for eight years. A confiscation hearing, to recover what might remain of the profits of the scam, is set to take place in November 2022.

MEET THE COUNTER FRAUD TEAM

Terry Smith

Director of Operations

T: 07971 895281

E: terry.smith@audit-one.co.uk

Rebecca Napper

Head of Operations (Proactive)

T: 07980 726 508

E: rebecca.napper@audit-one.co.uk

Michelle Watson

Head of Operations (Reactive)

T: 07580 589 024

E: michelle.watson@audit-one.co.uk

Paul Bevan

Counter Fraud Specialist

T: 07973 814 286

E: paul.bevan@audit-one.co.uk

Gemma Collin

Counter Fraud Support

T: 07920 590 180

E: gemma.collin@audit-one.co.uk

Martyn Tait

Counter Fraud Specialist

T: 07976 433 667

E: martyn.tait@audit-one.co.uk

Iain Flinn

Counter Fraud Specialist

T: 07973 814 207

E: iain.flinn@audit-one.co.uk

Stephen Veitch

Counter Fraud Specialist

T: 07973 814 475

E: stephen.veitch@audit-one.co.uk

Kathryn Wilson

Counter Fraud Specialist

T: 07973 814 205

E: kathryn.wilson@audit-one.co.uk

Simon Clarkson

Counter Fraud Specialist

T: 07980 729 654

E: simon.clarkson@audit-one.co.uk

David Wearmouth

Lead Investigation Officer

T: 07919 545 248

E: david.wearmouth@audit-one.co.uk

Gary Ross

Security Management Specialist

E: gary.ross@audit-one.co.uk

Tracey Moore

Investigator

E: tracey.moore1@audit-one.co.uk

Mel Potter

Investigator

E: mel.potter@audit-one.co.uk

FRAUD REPORTING HOTLINE

0191 441 5936

NATIONAL FRAUD REPORTING HOTLINE

0800 028 4060