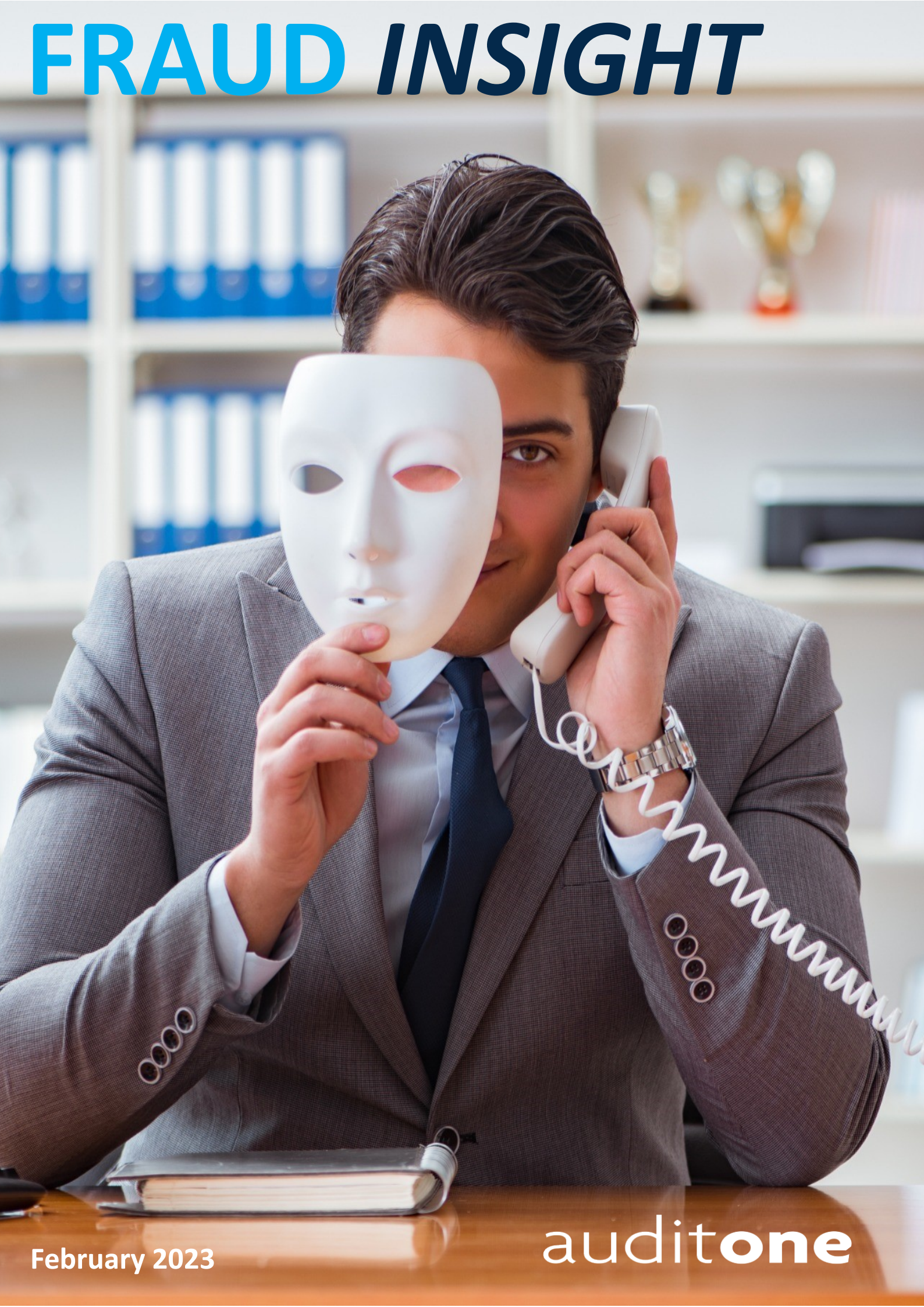
FRAUD INSIGHT



February 2023

auditone

BOGUS DOCTOR FACES FRAUD TRIAL

A “most accomplished fraudster” was paid between £1m and £1.3m by the NHS during the nearly two decades she posed as a qualified doctor after forging a degree certificate, a court has heard. Zholia Alemi, worked as a psychiatrist in the UK for 19 years after claiming to have qualified at the University of Auckland in New Zealand, a trial at Manchester crown court heard. The defendant is accused of 20 offences, including forgery and fraud, which she denies. Opening the case, Christopher Stables, prosecuting, said: “To put it bluntly, the defendant is a fraud. While she held herself out as being a doctor, she was utterly unqualified to do so.” Stables said Alemi forged a degree certificate and a letter of verification that is alleged to have come from the University of Auckland, which she then submitted to the General Medical Council (GMC) in 1995, with the aim of becoming a registered doctor in the UK. He said Alemi had deceived the GMC into accepting that she was a fully qualified doctor through “bogus assertions as to what her experience had been. Rather than passing her [medical] exams, she in fact failed them and was never qualified at all,” Stables said. “She had in fact secured entry on to the GMC register of medical practitioners but had done so by fraud; by forging her qualifications and other documents, which induced the GMC to accept her as genuine.” The court heard that Alemi had practised as a doctor in England, Scotland and Northern Ireland between 1998 and 2017, “quite literally the length and breadth of the country”, according to Stables. She denies 13 counts of fraud, three counts of obtaining a pecuniary advantage by deception, two counts of forgery and two counts of using a false instrument. The trial is expected to last four to five weeks.

Full article can be found here: https://www.theguardian.com/society/2023/jan/10/fraudster-posed-as-nhs-doctor-for-19-years-court-hears

---

CMA FINES FIRMS OVER £35M FOR NHS DRUGS ARRANGEMENTS

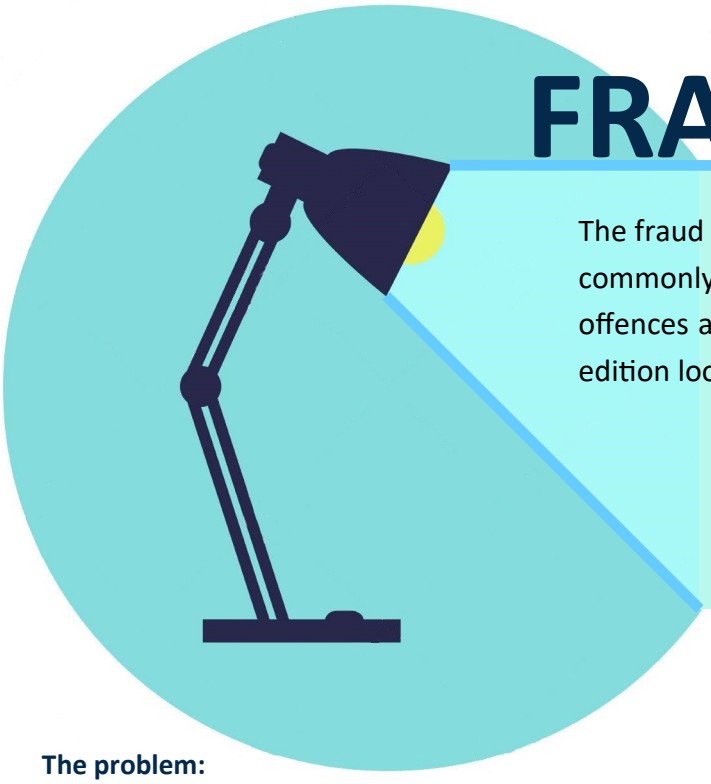
The Competition and Markets Authority (CMA) have issued fines to a number of pharmaceutical firms in relation to an arrangement under which a competitor was paid not to launch a product, and which enabled price increases to the NHS. From 2013 to 2017, the prices paid by the NHS for prochlorperazine rose from £6.49 per pack of 50 tablets to £51.68 – an increase of 700%. Consequently, between 2014 and 2018, the annual costs incurred by the NHS for prochlorperazine increased from around £2.7 million to around £7.5 million, even though the number of packs dispensed fell. The firms fined include Advanz, the private equity firm Cinven, and Lexon, all of which have been fined for breaking competition laws in previous pharmaceutical CMA investigations.

Andrea Coscelli, Chief Executive of the CMA, said:

“The size of the fines reflects the seriousness of this breach. These firms conspired to stifle competition in the supply of this important medication, so that the NHS – the main buyer of the drugs – lost the opportunity for increased choice and lower prices. While the arrangement was in place, the price increased significantly for a drug that people rely on to manage debilitating nausea, dizziness and migraines. All firms should know that we will not hesitate to take action like this against any businesses that collude at the expense of the NHS.”

Full details can be found here: https://www.gov.uk/government/news/cma-fines-firms-over-35m-for-illegal-arrangement-for-nhs-drug

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 this type of fraud. This edition looks at:

MANDATE FRAUD

The problem:

Mandate fraud is one of the fastest growing fraud risks that the NHS faces. UK finance estimate that in 2018/2019, over £93m was lost by businesses as a result of mandate and invoice fraud with an average loss of over £20k each time. It is feared the actual loss is significantly higher with some organisations choosing not to report the financial loss through fear of reputational damage.

How is this offence committed:

Supplier Bank Account Mandate Fraud

Someone contacts your business pretending to be one of your legitimate suppliers. They will often claim that they have changed bank accounts and ask for the system to be updated with the new bank details. If the changes are made, any subsequent payments will be made to the new fraudulent account and not the legitimate company who have never changed their account. This is often only identified when the legitimate company does not receive expected payments and queries this.

Standing Order Mandate Fraud

Someone contacts your business pretending to be from an organisation you have a standing order with. They will often ask you to change the standing order to reflect a change in their bank account details. If the changes are made any subsequent payments will be made to the fraudulent account. This is often only identified when the organisation doesn't deliver your products as they didn't get paid.

Payroll Mandate Fraud

Someone contacts your organisations payroll department pretending to be an employee and requests the bank account that their salary is paid into be changed. If the changes are made any subsequent salary payment are made to the fraudulent account. This is often only identified when the legitimate employee doesn't receive their salary and queries this.

How can mandate fraud risks be minimised

Suppliers:

- don't action changes based on emails or phone calls
- verify and corroborate any request to change suppliers' bank details using known information
- do not use any of the contact information within the email or click on any links within the email as these could be fake
- best practice would be to require the supplier to complete a detailed form to process the change. The counter fraud team can assist with setting up this process

Employees:

- payroll providers should have in place a formal processes that employees are required to follow to change bank accounts for salary payments
- don't action changes based on emails or phone calls
- verify and corroborate any request to change bank details by contacting the employee using a known method
- do not use any of the contact information within the email as these could be fake
- Maintain up to date records of standing orders and direct debits
- Check bank statements carefully for anything suspicious

If you have concerns regarding mandate fraud please contact your counter fraud specialist whose details can be found on the last page of this newsletter.

NATIONAL CASES: £2.1M AIR AMBULANCE FRAUDSTER JAILED

A man who created a false document in an attempt to steal more than £2 million intended for an air ambulance charity has been jailed for five years and three months for fraud and making a false statement on oath. In 2015, an elderly woman known to the subject was diagnosed with terminal cancer and sadly passed away at her home on 7 August 2016. The deceased wrote a will in 2014, making an air ambulance charity the main beneficiary of her estate. She left £25,000 to the subject who she had appointed as one of the executors of her will. Shortly before her death, the subject produced a document which he titled 'Letter of Wishes' to solicitors dealing with her estate, declaring that he was now the sole executor of the will and the main beneficiary. This meant that he suddenly stood to inherit £2,186,079, significantly more than the £25,000 which she had intended to leave to him in the 2014 will. Solicitors appointed to process the will raised doubts about the legitimacy of the letter of wishes and an investigation was launched.

It was found that the 75 year old subject wrote the letter of wishes shortly before the deceased passed away, and medical evidence from the deceased's GP confirmed that she did not have mental capacity when the letter was purported to have been signed by her. The subject involved two accomplices to support his criminal behaviour by requesting them to sign the letter of wishes as witnesses. These 2 men aged 35 and 42 provided sworn affidavits confirming that they signed the letter of wishes as witnesses before the victim passed away. However, they later confessed that they in fact signed the letter after the deceased had died. Both pleaded guilty to wilfully making a false statement on oath and were each given four month sentences suspended for twelve months and ordered to complete 60 hours of unpaid community work.

REGIONAL CASE: FRAUDSTER JAILED FOR £1.2M TRAVEL AGENT SCAM

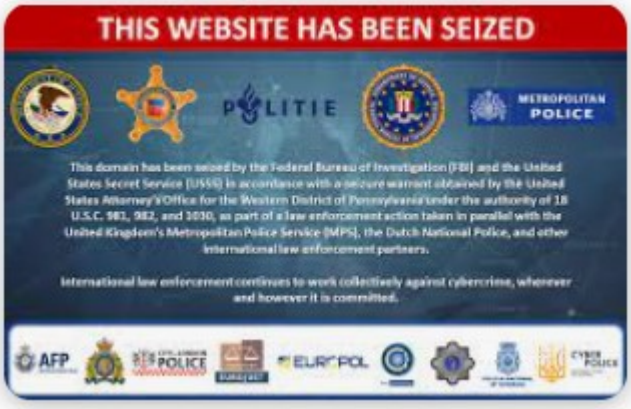
A heartless Stanley travel agent who claimed to have cancer during £1.2m holiday fraud has been jailed for 9 years. The 39 year old defrauded holidaymakers and even her own family and friends as part of an elaborate scam. Following the death of her dad from cancer, she decided to steal £520,000 from her own mother by taking over her financial identity. She also dissipated her mother's entire NHS pension and redirected her post and bank statements. As she drained her mother's cash, she also asked for loans from various other friends, often claiming she was being threatened, and gleaned thousands from her victims. At one point, she even tricked her mother into believing she was a millionaire - which she never was. As the money she stole from her mother slowly reduced, she decided to set up her own travel agency, and began defrauding other holidaymakers and friends. As a travel agent, she began offering trips to exotic locations such as Dubai, Asia and the Maldives for prices that seemed too good to be true funded by using money which was either her own, borrowed from family or friends, loaned from the bank, or were funds from previous holidays paid for by her victims. News of her offers quickly spread by word of mouth and on social media. Whenever she was approached by a potential customer about a holiday, she would then use normal websites which are accessed by any member of the public looking for a holiday and make

the deal very attractive by offering a discounted rate to her customers. Other holidaymakers only discovered when they reached the airport to find that despite having flight details, they did not have seats or that the booking had been cancelled because it had not been paid for. On numerous occasions she told unsuspecting customers that she was behind with her bookings due to her treatment for terminal cancer, which was a lie. She even took the drastic step of cutting her own hair and leaving it on her bed to further fool family members into thinking her hair was falling out due to the cancer. Durham Police said she presented herself as being frail, used a crutch and wore a headscarf when she was arrested in September 2020. Investigators made checks on her health to ascertain if she was well enough to be questioned and her medical records revealed she had never had cancer treatment. The court heard the subject's offences came to light when numerous victims began bombarding Durham Constabulary with calls. The calls caused such unprecedented demand on police call handlers, complaints had to be directed to an email account which was quickly set up to deal with what was happening. It quickly turned into the constabulary's biggest ever fraud case. The subject had pleaded guilty to ten charges of fraud, one charge of theft and one charge of concealing, converting, and transferring criminal property at a previous hearing. Sentencing her to 9 years imprisonment, the judge said that the subject presented herself as "charming and engaging" but "mercilessly abused the trust of your nearest and dearest". She branded her a "callous individual" and added that she had an "extraordinary talent for dishonesty".

NATIONAL CASE: £122M FRAUD PROBE IN NHS WALES

A multi-million pound fraud investigation has begun at Wales' largest health board. Specialist investigators have been called in to Betsi Cadwaladr University Health Board after auditors discovered at least £122m was allegedly not properly accounted for. Audit Wales is also conducting a "high level review of board effectiveness" to understand what went wrong and how. Issues were first uncovered in early 2022 when auditors found a number of "significant errors" in the health board's account for the 2021-22 financial year. They allegedly found there was £72m of unpaid invoices and bills listed in the accounts but could not find evidence that they existed. Overall, auditors are said to have raised concerns that £122m of expenditure was not properly accounted for. Accountancy and consulting firm EY were commissioned to review the accounts after auditors raised concerns. Following their report, the NHS Counter Fraud Service Wales was asked to investigate.

LARGEST EVER FRAUD OPERATION: ISPOOF



An international one stop spoofing shop has been taken down in the UK's biggest ever fraud operation, led by the Metropolitan Police. More than 200,000 potential victims in the UK alone have been directly targeted through the fraud website iSpoof. At one stage, almost 20 people every minute of the day were being contacted by scammers hiding behind false identities using the site. They posed as representatives of banks including Barclays, Santander, HSBC, Lloyds, Halifax, First Direct, NatWest, Nationwide and TSB. Scotland Yard's Cyber Crime Unit worked with international law enforcement, including authorities in the US and Ukraine, to dismantle the website this week. iSpoof enabled criminals to appear as if they were calling from banks, tax offices and other official bodies as they attempted to defraud victims. Victims are believed to have lost tens of millions of pounds while those behind the site earned almost £3.2 million in one 20 month period.

iSpoof allowed users, who paid for the service in Bitcoin, to disguise their phone number so it appeared they were calling from a trusted source. The average loss from those who reported being targeted is believed to be £10,000. In the 12 months until August 2022 around 10 million fraudulent calls were made globally via iSpoof, with around 3.5 million of those made in the UK. Losses reported to Action Fraud as a result of the calls and texts via iSpoof is around £48 million. Because fraud is vastly underreported, the full amount is believed to be much higher. Detective Superintendent Helen Rance, who leads on cyber-crime for the Met, said: "By taking down iSpoof we have prevented further offences and stopped fraudsters targeting future victims. Our message to criminals who have used this website is we have your details and are working hard to locate you, regardless of where you are."

SCAM ALERT: COURIER FRAUD—NEW TACTICS

The warning comes as a new list of tactics used by courier fraudsters has been unveiled by the City of London Police. Typically, courier fraudsters target their victims by claiming to be a police officer or a member of staff from a victim's bank and they often pressure people into making quick financial decisions to assist with fictitious investigations. In 2021 alone, 3,625 people were victims of courier fraud, with loses totalling more than £15.2 million.

Four common MOs used by courier fraudsters

- **Bank card expiry:** Fraudsters claim to be from the victim's bank and say their card is no longer valid. They ask for the PIN number and then send a 'courier' to collect the card before using it for fraudulent purposes
- **Purchasing high end items:** The suspects pretend to be police officers and ask the victim to help with an undercover operation by purchasing expensive items like watches, jewellery and gold. Once the item is bought, the victim will hand over the item to the criminal
- **Counterfeit cash/bank investigation:** A person claiming to be a police or banking official informs the victim that they need to help with a banking corruption investigation. The victim is told to withdraw a large amount of money and the cash is picked up later by a courier to 'check for fingerprints or to identify counterfeit bank notes'
- **Computer takeover:** The fraudster telephones the victim, purporting to be from their internet service provider, saying that they have had an issue with their internet connectivity and they are due compensation. The victim is persuaded to download a remote access application, giving the suspects access to their home computers. The fraudster persuades the victims into thinking that they have been paid too much compensation and the victims then withdraw cash to pay the money back, which is later collected by a courier

Take Five To Stop Fraud advice

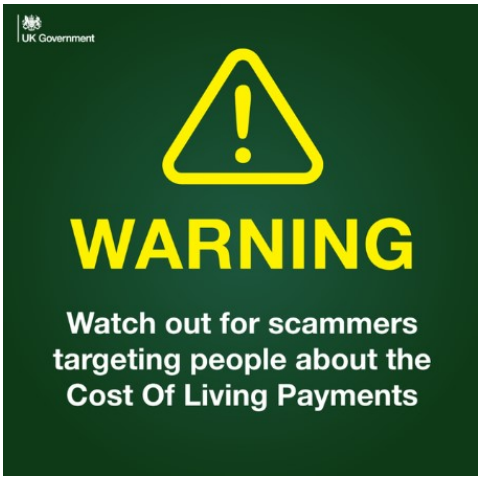
- **Stop:** Taking a moment to stop and think before parting with your money or information could keep you safe.
- **Challenge:** Could it be fake? It's okay to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.
- **Protect:** If you think you've been a victim of fraud,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

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

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

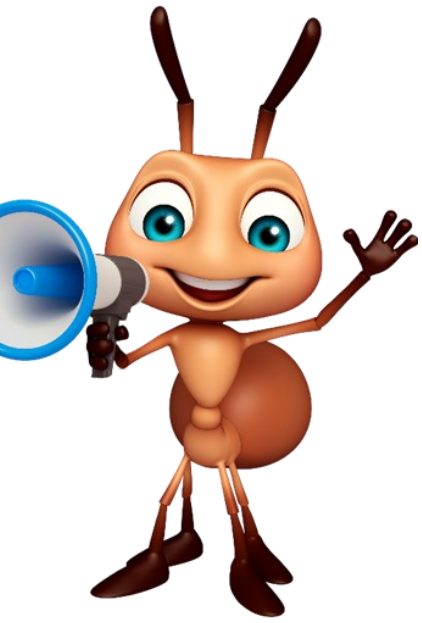
Councils across the nation have urged households not to give out their bank or card details over the phone if they get a call about the £150 council tax rebate. The MSE website said: "In most cases, the rebate is paid automatically to those who pay their council tax by direct debit - and most people 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?

One of the best ways of helping the NHS prevent fraud is to know what to look out for in your day to day job. One good way of doing this is to arrange a fraud awareness presentation for your team, department/ward or directorate. Our team of trained counter fraud specialists will provide you with an interactive presentation focusing on real life fraud cases. The presentations 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. To arrange a presentation, please click the icon below, complete the form and one of our team will be in touch.

Presentation Request form - Click here >>>>>>

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

Sarah McCloud

Counter Fraud Specialist

T: 07973 814 317

E: sarah.mccloud@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

Steven Sherwood-Hodgson

Counter Fraud Specialist

T: 07977 065 338

E: steven.sherwood-hodgson@audit-one.co.uk

FRAUD REPORTING HOTLINE

0191 441 5936

NATIONAL FRAUD REPORTING HOTLINE

0800 028 4060