FRAUD INSIGHT

JULY 2023

auditone

NATIONAL CASE: HOSPITAL MANAGER CONVICTED OF FRAUD

A hospital theatre manager has been jailed for 11 years for his part in a "sophisticated" fraud that cost the NHS £600,000. Hasan Abusheikha, 47, took bribes and stole equipment that had been donated to the West Herts NHS Trust. The former St Albans City Hospital worker was investigated by the NHS Counter Fraud Authority. Prosecutors said his crime *"involved a significant undermining of the proper function of a public service".* His trial

at St Albans Crown Court heard Abusheikha, of Church Street in Hemel Hempstead, had worked at the hospital for more than 10 years and was able to procure medical equipment on behalf of the trust. As part of the role, he was required to make purchase order requests for items required for surgical procedures carried out within the hospital. He was found guilty of theft, fraud and bribery. Co-defendant Elmo Emanuel, 74, of Station Road in Wingate, County Durham, ran medical equipment suppliers Implants International and Xtremity Solutions, and was also convicted of bribing Abusheikha and was jailed for 28 months. Another trust supplier, Jawid Khan, 51, Windmill Road, Hemel Hempstead, admitted bribe charges and was handed an 18-month suspended sentence. He must carry out 200 hours of unpaid work. Prosecutor James Brown said Emanuel bribed Abusheikha with £10,000 - over a period of five years - for sales of over £200,000. The money was paid into Abusheikha's brother's bank account in Jordan, he told the court. He said Khan had also paid a bribe of £2,082 into Abusheikha's bank account over 15 months for £21,228 worth of sales. Mr Brown said: *"He was in a position of procurement. It was payment for access. The money had a purpose to buy some influence. He seemed to be trusted and was proactive about procurement issues."* Medical equipment costing in excess of £65,000, including surgical instruments, were recovered after a search of Abusheikha's house. David Burgess, defending, said Abusheikha was a loyal and devoted employee for most of his 10 years. Sentencing, Judge Lana Wood said: *"The earning of commission was your primary objective. "Your primary concern should have been the best interests of the trust."* A confiscation hearing will take place at a later date.

WATCH OUR VIDEOS

AuditOne has a range of videos highlighting the types of frauds that commonly occur in the NHS. Why not take a look:

Click here to access videos

TICKET TO NOWHERE

Action Fraud, the national reporting centre for fraud and cybercrime, is warning the public to be careful when buying tickets for a range of sport, music and comedy events, as new figures reveal over **£6.7 million was lost to ticket fraud in 2022.**

Pauline Smith, Head of Action Fraud, said:

"Action Fraud has seen a rise in ticket fraud over the past twelve months, as criminals take advantage of people wanting to enjoy more live sport and music. We urge people to be wary of ticket sales from unknown websites or people they do not know. Criminals may offer deals on sold-out or exclusive events, however once you have parted with your money, the tickets are either fraudulent or never appear at all. Remember, if it sounds too good to be true, it probably is."

How to protect yourself from ticket fraud:

- Only buy tickets from the venue's box office, official promoter or agent, or a well-known ticketing website.
- 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 the money if you become a victim of fraud.
- The password you use for your email account, as well as any other accounts you use to purchase tickets, should be different from all your other passwords. Use three random words to create a strong and memorable password, and enable 2-step verification (2SV).
- Be wary of unsolicited emails, texts or adverts offering unbelievably good deals on tickets.
- 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 visit star.org.uk/buy_safe.

NATIONAL CASES: FAMILY SENTENCED FOLLOWING £2M HEALTH INSURANCE SCAM

Two brothers have been jailed and their parents given suspended sentences over a £2m health insurance scam. The website con misled people into needlessly paying for European Health Insurance Cards, freely available from the official NHS website.

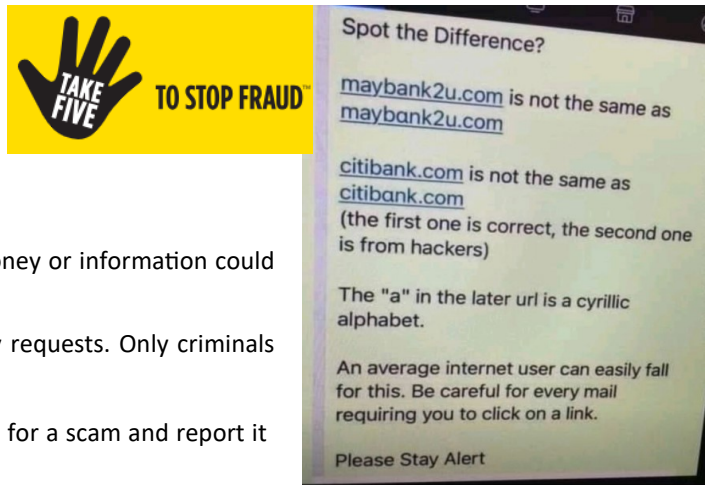
The defendants, all from Sunderland, were sentenced at Leeds Crown Court in June 2023.

The investigation was led by Trading Standards working alongside North Yorkshire and City of York councils. The swindle saw Damien Sartip Zadeh, 32, and Dale Sartip Zadeh, 35, push their misleading websites to the top of internet search results, to trick consumers into needlessly paying for their health cards. However, the websites were a front for what was described by City of York Council as a "clever cut and paste" job, with customers' details simply being copied over into the NHS website form. Both Damien Sartip Zadeh, of Angram Drive, Sunderland, and his brother Dale, were found guilty of fraudulent trading and laundering the proceeds, between February 2013 and October 2019. The pair were jailed for nine-and-a-half years and eight years respectively.

Their parents, Diane Sartip Zadeh, 60, and Mahmud Sartip Zadeh, 62, also of Angram Drive, Sunderland, were found guilty of money laundering and were sentenced to two years in prison, suspended for two years. Both were also told to attend 10 activity rehabilitation days, with Mahmud Sartip Zadeh ordered to carry out 200 hours of unpaid work. The brothers were directors of the companies behind the misleading websites. They were disqualified from being directors for 10 years. Damien Sartip Zadeh was also convicted of engaging in aggressive commercial practices after threatening consumers who complained to prevent them pursuing refunds. Lord Michael Bichard, who chairs National Trading Standards, said: *"This was a case of serious and organised fraud, where large sums were taken from unsuspecting, ordinary, busy people and the sites were a scam from start to finish."* Ruth Andrews, eCrime manager at City of York Council, added: *"Despite multiple warning flags being raised with these defendants they brazenly persisted with their fraud."* Councillor Greg White, executive member for regulatory services at North Yorkshire Council, commended the National Trading Standards eCrime team for bringing *"this long and difficult case against this family of scammers to its successful end"*.

QUICK TIP: SPOT THE DIFFERENCE?

Scamsters are constantly looking at new ways to deceive and steal peoples money. The image to the right is quick tip to help keep you safe:



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 ok to reject, refuse or ignore any requests. Only criminals will try to rush or panic you.

PROTECT Contact your bank immediately if you think you've fallen for a scam and report it to Action Fraud.

LOCAL CASES: CHARITY TRUSTEE CONVICTED OF FRAUD

A North Yorkshire ex-charity trustee has walked free from court despite pocketing almost £27,000 from a privatised probation organisation.

Hugh Morgan Williams took £26,966 from Durham and Tees Valley Community Rehabilitation Company (CRC) while he was chairman. The Cabinet Office may now decide his conviction could mean he should forfeit his OBE, which was granted in June 2008.

Teesside Crown Court heard how the 70-year-old used personal contacts with a private company he had links to, to procure contracts for DTVCRC and took ten per cent of the contract value for his own personal use without the knowledge of the board. During the investigation, it was discovered that Williams had attempted to have entries deleted on invoices with the name DTVCRC on them prior to his invoices being submitted to the company for payment. Williams, of North Riding Rise, Thornton-le-Moor, near Thirsk, pleaded guilty to fraud between January 1, 2015, and February 1, 2016, relating to his time at the CRC, during a brief hearing. He received an OBE in June 2008 for services to business in the North East and North Yorkshire Police has confirmed that the honours department of the Cabinet Office have been made aware of his hearing with a view to a request to have this forfeited. The officer in charge of the case, Detective Constable Fraud Investigator, Emma Harris said: *"Mr Morgan Williams was trusted with money from the public purse. He has abused the trust placed on him to safeguard the interests of DTVCRC and his position in order to make financial gain for himself. This sends a message that no matter what your position, if you commit these offences, you will be found out and brought to justice."* Morgan-Williams was sentenced to 17 months in prison suspended for 12 months. He was appointed non-executive chair of the Durham and Tees Valley Community Rehabilitation Company in 2015. Charges relating to his time as a trustee of Cowesby Charity, which helps people in and around Cowesby near Thirsk, were dropped by the prosecution. The disgraced former charity trustee was also previously chairman of the Northumberland, Tyne and Wear NHS Foundation Trust.

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.

Why not add something different to the next team meeting?

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

Victims reported losing a total of £15,319,057, a 41 per cent increase on last year's results, which amounts to an average loss of £2,372 per victim. From May – August alone, more than £4.6m was lost. With the summer months seeing the highest levels for holiday fraud reports, Action Fraud has launched a national awareness campaign today to urge the public to think twice before booking a holiday, so consumers don't get burnt before they are on the beach. Pauline Smith, Head of Action Fraud, said:

"With summer only just around the corner, we enter a period where fraudsters ramp up efforts to catch out unsuspecting members of the public. Scammers prey on people wanting to find a good deal online – whether that's cheap flights, great hotels close to the beach at discounted rates or package holidays that undercut well-known travel operators and brands, people are more than willing to snap up a deal which sometimes comes at a heavy cost. When booking a holiday here or abroad, it's important to do your research before handing over any money and to double check any website. To avoid the wave of crime this summer we encourage people to stop, check and research before paying. If it sounds too good to be true – it most definitely is."

Anna Bowles, Head of Consumers and Enforcement at the UK Civil Aviation Authority, which runs the ATOL financial protection scheme, said:

"Before booking any trip abroad it is always worth doing some homework before you part with any money to make sure you limit your risk of being impacted by fraud. Make sure you research the company you're booking through - check reviews and ensure that your booking includes all the extras you're expecting, such as baggage allowance and transfers. We also recommend some simple measures to financially protect your well-earned holiday, including using the atol.org website to check your trip is financially protected by ATOL, consider paying by credit card and taking out travel insurance as soon as you book. This will add extra layers of protection against anything going wrong with your booking."

Data revealed that the top 10 hotspots of people being caught out by holiday fraud in the UK were as follows: London, West Midlands, Greater Manchester, Thames Valley, West Yorkshire, Hampshire, Essex, Sussex. Avon and Somerset and Kent. Interestingly, People in their 20s and 40s who reported losses accounted for 44 per cent of all reports, further dispelling the myth that only older people are targeted by fraudsters. Holiday fraud encompasses many different tactics employed by criminals to dupe unsuspecting members of the public. The most frequent frauds are clone comparison websites, airline websites and holiday websites. At a quick glance it would appear you are on a trusted site, whereas in reality the URL has been changed. Here, victims assume they are on the genuine site and willingly hand over money at a great cost. Fake confirmation emails or booking references are even sent, which has resulted in some cases of victims only realising they have fallen victim to fraud when they are at the airport to check in for their flight to be told that their booking does not exist.

An emerging trend is fraudsters using counterfeit Air Travel Organisers' Licensing (ATOL) protect numbers on their fake webpage. All credible and trusted companies are provided with a number that shows the company has passed the regulatory checks by ATOL, with this number being unique to the website. Recently, fake websites have used duplicate or fabricated numbers which have been edited onto an ATOL logo. ATOL recommends double checking all numbers on websites and with travel operators before handing over any money. If you do pay, use a credit card as this can offer greater protection should you lose your money.

Top tips to avoid falling victim to holiday fraud

- **Do your own research:** Booking your trip via a company you haven't used before? Do some research to check they're legitimate. Read feedback from sources that you trust, such as consumer websites. You can find a company's official website by searching for them on Google or another trusted search engine.
- **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 ATOL or CAA website.
- **Pay safe:** Book your holiday with a credit card, if you have one. Most major credit card providers protect online purchases, and are obliged to refund you in certain circumstances. Using a credit card (rather than a debit card) also means that if your payment details are stolen, your main bank account won't be directly affected
- **Secure your email:** If your email is hacked, it could allow a criminal to access information about your holiday booking. Use 3 randoms words to create a strong password for your email that's different to all your other passwords. If you're offered 2-step verification to protect your email and social media accounts, always use it.

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

Criminals are using the cost of living crisis to scam the public. Don't become a victim

Law enforcement, government and private sectors partners are working together to encourage members of the public to be more vigilant against fraud, particularly about sharing their financial and personal information, as criminals seek to capitalise on the cost of living crisis. Criminals are experts at impersonating people, organisations and the police.

Energy Bill Rebates

Between September 1, 2022 and November 13, 2022 Action Fraud received over 350 reports relating to fake text messages and emails purporting to be from the UK Government. The messages state that the recipient is "owed" or "eligible" for an energy bill discount as part of the Energy Bill Support Scheme.

Although the content of messages can vary, a significant number of emails are titled "Are you Eligible to Apply for Energy Bill Rebate" or "Government energy rebate scheme", with a header in the email body stating "E.ON: Gas and electricity supplier". Some emails include the Ofgem logo in an attempt to legitimise the correspondence.

The links in the emails and texts lead to genuine looking websites that are designed to steal personal and financial information. Households in the UK do not need to apply for the Energy Bill Support Scheme and you will not be asked for your bank details. If you have spotted a suspicious text message, please forward it to 7726. If you have received an email which you're not quite sure about, you should forward it to: report@phishing.gov.uk

In recent months, people have reported receiving suspicious phone calls from fraudsters claiming to be from their bank or the police. The scammer warns the recipient that several suspicious transactions have been made on their

account related to scam government energy rebates and asks them to transfer their funds into a 'safe account'.

Remember, your bank or the police will NEVER ask you to transfer money or move it to a safe account.

Cost of Living Payments

Since its announcement in May, fraudsters have been seeking to capitalise on coverage related to the government's cost of living scheme, which offers £650 to millions of low income households. The Department for Work and Pensions has issued a warning about scams related to cost of living assistance following reports of scam phone calls, emails and text messages. In one such example, the recipient is asked to claim or apply for the payment by registering via a link. The links in the emails and texts lead to genuine looking websites that are designed to steal personal and financial information. Please remember, if you are eligible for cost of living assistance, you do no need to apply for the payment or contact the DWP directly. Payment to you is automatic and the DWP will never ask for personal details by SMS or email. More information is available here.

Fuel vouchers, phone bill discounts and supermarket offers

There has been a rise in consumers being targeted by phishing emails pretending to be from utility companies claiming to provide savings on energy bills, as well as offering fuel vouchers, phone bill discounts and supermarket offers. These emails are becoming increasingly sophisticated and are designed to harvest personal and financial information. A number of supermarket brands have been spoofed in fake ads on social media with offers of too good to be true deals, competitions or giveaways. A number of people have reported seeing fake ads offering free food products that are due to expire. The ad encourages people to register via a link in order to win or claim the food. In reality, the offer does not exist and the third party website is designed to steal your personal or financial information. In recent months, a number of people have reported receiving suspicious phone calls from scammers claiming to be from their phone provider. The scammer states that the phone owner is eligible for a discount on their phone bill due to cost of living hardships and then asks a series of questions designed to steal their personal information. If you see an offer that sounds too good to be true, it probably is. Always check the brand's official website or social media channels to verify whether an offer is authentic. You can report suspicious phone calls to Action Fraud here: Report.

Fake investment opportunities

Money laundering and other financial crimes are on the rise as scammers continue to prey on people looking to save as much money as they can or offset rising costs by making investments that promise high returns. There are many different types of investment fraud, which usually involve criminals contacting people out of the blue and convincing them to invest in schemes or products that are worthless or do not exist. Once the criminals have received payment, they cease contact with the victim. Fraudsters are using a range of social media platforms to contact people with offers of non-existent bank refunds. In many cases, the fraudster shares a fake screenshot showing amounts ranging from £1,289 to £1,855 being deposited into an account. This is intended to encourage the

recipient to share their bank details and claim a refund. In reality, no refund exists and the scammer will use your financial information to steal money.

- **How to protect yourself from financial investment fraud:**

  Investment opportunities: Don't be rushed into making an investment. Remember, legitimate organisations will never pressure you into investing on the spot.

- **Seek advice first:** Before making significant financial decisions, speak with trusted friends or family members, or seek professional independent advice.

- **FCA register:** Use the Financial Conduct Authority's (FCA) register to check if the company is regulated by the FCA. If you deal with a firm (or individual) that isn't regulated, you may not be covered by the Financial Ombudsman Service (FOS) if things go wrong and you lose your money.

For more information about how to invest safely, please visit: https://www.fca.org.uk/scamsmart

SCAM ALERT: WhatsApp ACCOUNT TAKE OVER

Action Fraud has received over 60 reports relating to a scam that steals access to a WhatsApp user's account. The scam begins when a criminal gets access to another WhatsApp account which has you listed as a contact. The criminal, posing as your friend or someone that's a member of a WhatsApp group you're in, will then send you seemingly normal messages to try and start a conversation with you.

However, around the same time you will receive a text message from WhatsApp with a six-digit code. This is because the criminal has been trying to login to WhatsApp using your mobile number. The criminal will claim that they sent you their code by accident and ask you to help them by sending it to them. Once the criminal has this code, they can login to your WhatsApp account and lock you out. The criminal will then use the same tactic with your WhatsApp contacts in an effort to steal more accounts and use them to perpetrate fraud.

What you need to do

- Set up two-step verification to give an extra layer of protection to your account: Tap Settings > Account >Two-step verification > Enable.
- THINK. CALL. If a family member or friend makes an unusual request on WhatsApp, always call the person to confirm their identity.
- Never share your account's activation code (that's the 6 digit code you receive via SMS)
- 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.

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

Martyn Tait

Counter Fraud Specialist

T: 07976 433 667

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

Gemma Collin

Counter Fraud Support

T: 07920 590 180

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

Laura Fox

Lead Investigation Officer

T: 07976 759 637

E: laura.fox@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

Paul Bevan

Counter Fraud Specialist

T: 07973 814 286

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

Steven Sherwood-Hodgson

Counter Fraud Specialist

T: 07977 065 338

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

Michelle Acuna-Ocana

Lead Investigation Officer

T: 07974 096 752

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

FRAUD REPORTING HOTLINE

0191 441 5936

NATIONAL REPORTING HOTLINE

0800 028 4060