Fraud Counts Newsletter

Summer 2023

Introduction

Welcome to our latest edition of our Counter Fraud Newsletter for NHS staff.

This newsletter contains information on an NHS staff member stealing £500,000, an iSpoof website shut down by Scotland Yard, a family who made over £2 million using misleading websites to trick people into paying for European Health Insurance Cards, file sharing scams, salary diversion fraud, and how to contact your Local Counter Fraud Specialist.

Fraudster stole £500,000 from NHS



Thomas Elrick pictured leaving Harrow Crown Court (Image: Newsquest)

Thomas Elrick was the Assistant Managing Director for Planned and Unscheduled Care at Harrow Clinical Commissioning Group (CCG) where he had the authority to approve invoices up to £50,000. He abused his position to steal over £500K to fund his lavish lifestyle and even tried to use his late wife's email account to cover his tracks. She had died eight years previously.

Between August 2018 and December 2020, he authorised payments totalling £564,484 to a company called Tree of Andre Therapy Services Limited. The company was registered in Scotland under Elrick's husband's name and the money was paid into a bank account registered to himself.

He was the sole approver of the invoices and no services were delivered for the CCG by Tree of Andre. His fraudulent activities were revealed when a colleague queried invoices and found that Tree of Andre was not registered on the Care Quality Commission (CQC) website.

The NHS Counter Fraud Authority said: "The money defrauded was used to enjoy the lifestyle he had become accustomed to and that he wanted more. The fraud had become an addiction and he was aware that he would be caught."

Elrick pleaded guilty and is awaiting sentencing at Harrow Crown Court.

©ASW Assurance

Scotland Yard shuts down iSpoof website, which helped scammers steal using fake bank phone calls



Picture: Metropolitan Police

Tejay Fletcher of London was sentenced at Southwark Crown Court (May 2023) for 13 years and four months after entering an early guilty plea to the charges of making or supplying articles for use in fraud, encouraging or assisting the commission of an offence, possessing criminal property and transferring criminal property.

The largest fraud investigation led by the Metropolitan Police supported by national and international law enforcement partners, resulted in the bringing down of the website police describe as a "one-stop spoofing shop" used by scammers to steal tens of millions of pounds from Britons via fake bank phone calls.

Fletcher was the leading administrator of ispoof.cc, an online shop from which fraudsters could buy the tools to carry out their criminal trade by paying for a subscription. In exchange for monthly subscriptions, iSpoof provided its users with services which included the ability for its subscribers to use a caller ID 'spoof' to appear as if they were calling victims from a bank or other trusted organisations. Using iSpoof services, criminal users could call unsuspecting bank customers pretending to be genuine employees and, with the assistance of other iSpoof tools, obtain passwords, PIN codes, and then access customers' bank accounts and empty them.

The total losses to victims of frauds enabled by iSpoof in the UK exceeds £43 million, with the total global losses estimated to be at least £100 million. The amount received from users in iSpoof subscriptions and then paid out to Fletcher and others linked to iSpoof was 112.6 Bitcoin (BTC), or approximately £3.2 million.

Fletcher received by far the largest share of the profits of iSpoof, receiving at least £1.3 million from the fraudulent site. The Crown Prosecution Service intends to use confiscation proceedings to prevent Fletcher from profiting from his crimes – read more here.



If you have any suspicions or concerns,
You can call us anonymously on

0800 028 40 60

POWERED BY **CRIMESTOPPERS**

Or search 'NHS Fraud' online for more information

The NHS Counter Fraud Authority leads on fighting fraud, bribery and corruption in the NHS and the wider health group

NHS
Counter Fraud Authority

Department of Health & Social Care

Family who pocketed £2m from website scam sentenced to 21 years



Picture: National Trading Standards

A family made over £2 million using deliberately misleading websites to trick people into paying for European Health Insurance Cards (EHICs), which were freely available from the official NHS website.

The scammers used a computer programme to push their misleading websites to the top of internet search results to deceive consumers into needlessly paying for their EHIC. When customers realised they had been duped into paying for a free service, complaints were met with hostility and aggression.

Requests from victims to cancel or receive a refund (which they were legally entitled to) were refused and often followed-up with the threat of legal action if they attempted to claim a chargeback from their bank or credit card company.

Damien and Dale Sartip were sentenced in May 2023 at Leeds Crown Court to nine-and-a-half years and eight years respectively after being found guilty of fraudulent trading and laundering the proceeds between 2013 and 2019.

Damien Sartip was also convicted of engaging in aggressive commercial practices after threatening consumers who complained to prevent them pursuing refunds.

The brothers have both been disqualified from being directors for ten years.

Their parents were found guilty of money laundering and were sentenced to two years, suspended for two years. Both are also required to attend 10 activity rehabilitation days. Mahmud Sartip Zadeh was also ordered to carry out 200 hours of unpaid work and disqualified from being a director for five years.

Note to readers - since Brexit, the EHIC has been replaced by the Global Health Insurance Card (GHIC).

You can use your EHIC when abroad in Europe until it expires and then apply for the GHIC by clicking here. A UK GHIC and new UK EHIC are free of charge.

Suspicions of Fraud and Bribery may be reported anonymously by telephoning the NHS Reporting Line in confidence - 0800 028 40 60 or www.reportnhsfraud.nhs.uk



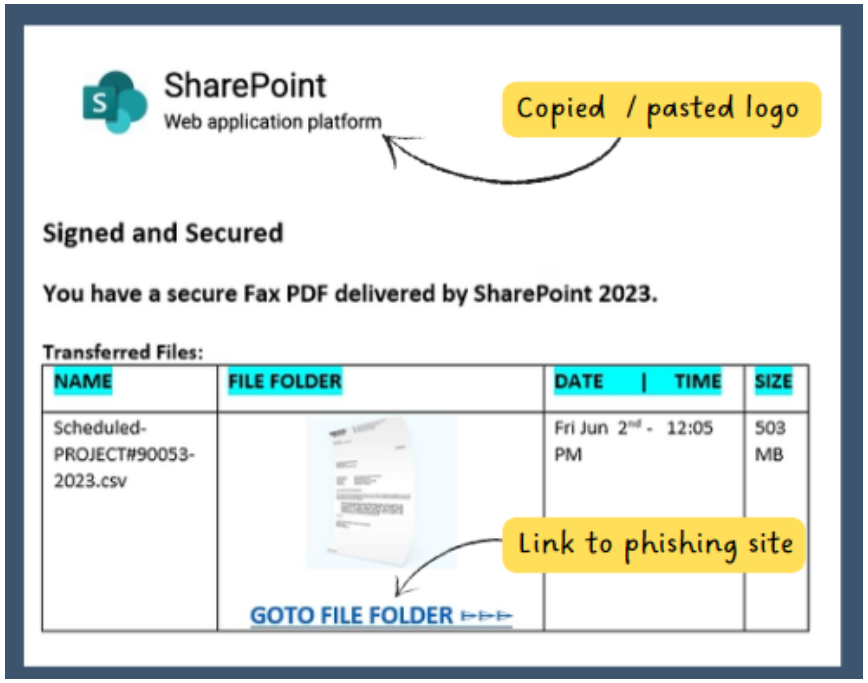
©ASW Assurance

Cyber security

File sharing scams

Phishing emails are often the first step in a fraud attempt. They are designed to trick you into taking action that isn't required - whether that is sharing your log in credentials, making a payment, or disclosing personal or sensitive data. Fraudsters can impersonate NHS colleagues and external partners to try and trick us into taking unnecessary action.

We have recently seen an increase in phishing emails encouraging receivers to click on a link to view a document within SharePoint. SharePoint is a genuine application which is part of Microsoft Teams which allows documents to be shared and managed amongst users. Fraudsters are emailing NHS staff with a mock SharePoint invite, like the one shown below.



If the recipient clicks on the link, it will ask them to "log in" to SharePoint with their NHS credentials. The person's email address and password will be harvested and used for criminal purposes. Clicking the link may also allow malware to be transferred to NHS systems.

To add credibility to these emails, the fraudster may hack into genuine NHS email accounts and use those accounts to send their phishing emails, making them appear to come from a genuine NHS employee.

Prevention Advice

- If you receive an email like this which you are not expecting and do not know the sender (even if they appear to be a genuine NHS employee), do not click on the link. Either contact your IT department or report to spamreports@nhs.net.
- If you do know the sender, give them a call on their official contact number or on Microsoft Teams to check if the link is genuine. Don't rely on any contact details within the email as these may belong to the fraudster.

©ASW Assurance

Salary diversion fraud



Following reports in the press that many NHS staff will receive backdated pay in June, there is an increased risk that fraudsters may try and divert salary payments.

Salary Diversion Fraud often works in a similar way to the Share Point phishing email shown above.

Instead of sharing a link to a "secure file" the fraudster sends a link which they claim is for ESR. They often claim that there has been a problem with payroll or that the person's bank details are causing an issue.

This is intended to make the recipient feel anxious, and to click on the "link to ESR" without checking it is safe.

If you hover over the link with your mouse, you should be able to see the web address that it will really take you to.

If you click on the link, you will see a fake ESR page. If you enter your log in credentials, they will be stolen by the fraudster. They can then use your log in to amend your bank details.

Prevention Advice

- If you get any emails directing you to log into ESR, open a web browser and type in the address manually (https://my.esr.nhs.uk).
- ESR is set up so that if your bank details change, or if a new assignment is added to your profile, you will get an automated email from esr.wfmPROD@nhs.net. If you get an email from this address saying a change has been made and you didn't request it, or if you are not due to start a new assignment, please contact Payroll immediately.
- Use a strong and unique password for ESR.
- Use the strongest privacy settings available on social media accounts.

©ASW Assurance

Our Local Counter Fraud Team

Our Local Counter Fraud Specialists are fully accredited with the University of Portsmouth. We aim to prevent and deter fraud and hold those to account who commit fraud against the NHS. Counter Fraud Services are provided by ASW Assurance (www.aswassurance.co.uk), an NHS consortium providing counter fraud and internal audit services to NHS and healthcare organisations.

If you would like to know more about our Counter Fraud work or arrange for your department to receive a Fraud Awareness Presentation, please contact one of our team below.



Gareth Cottrell – Counter Fraud Manager

✉ gareth.cottrell@nhs.net ☎ 01872 258057
07814 002364



Tracy Wheeler – LCFS

✉ tracy.wheeler2@nhs.net ☎ 01752 431378
07789 868568



Byron Kevern – LCFS

✉ byron.kevern@nhs.net ☎ 07775 417508



Sarah Smith – LCFS

✉ sarah.smith337@nhs.net ☎ 07467 685609



Sandra Bell – LCFS

✉ sandra.bell19@nhs.net ☎ 07467 685529

©ASW Assurance