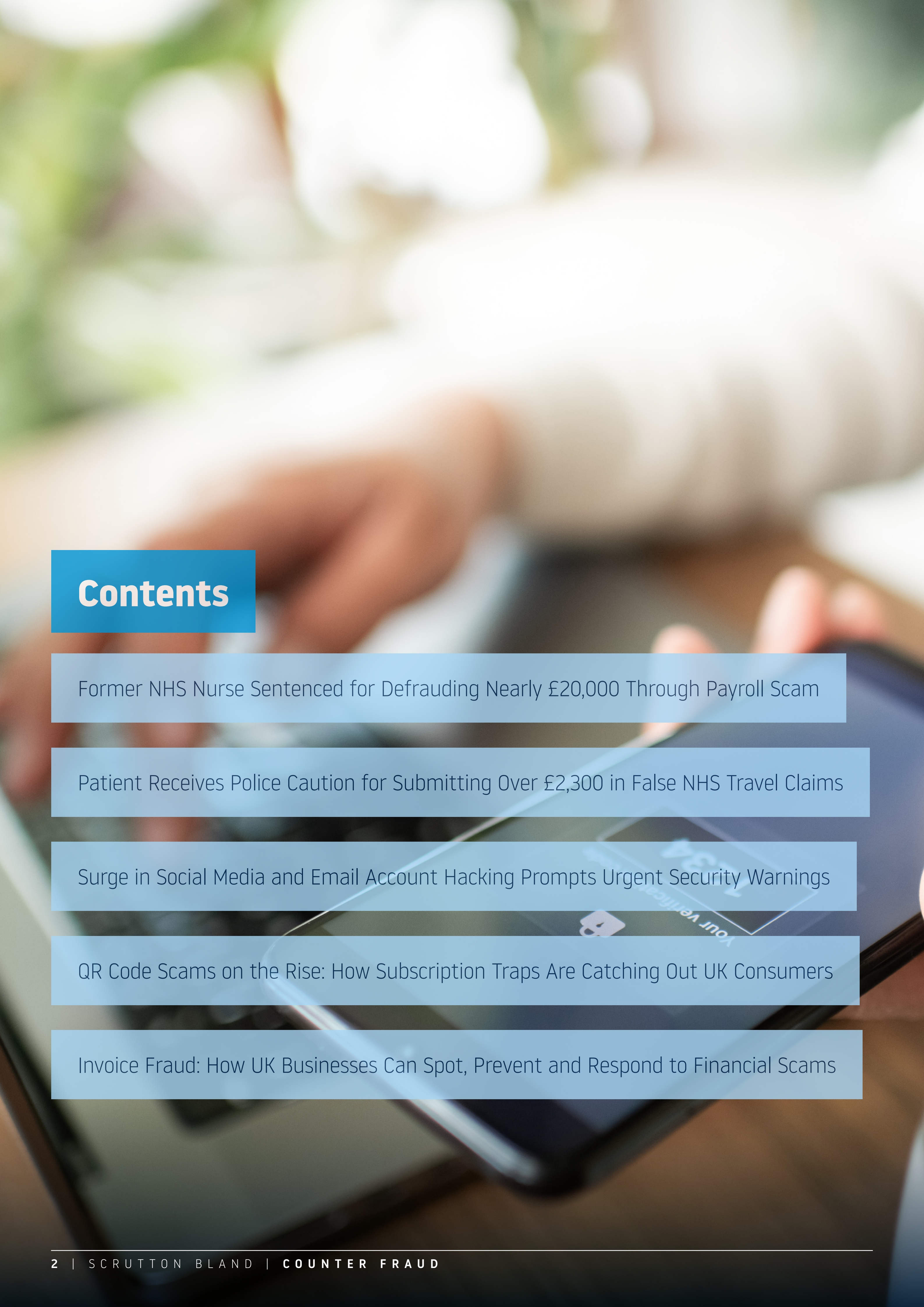
scruttonbland

Part of the SUMER Group

scruttonbland.co.uk

COUNTER FRAUD NEWSLETTER

FOR THE HEALTH AND SOCIAL CARE SECTOR



Contents

Introduction

Welcome to our Spring Counter Fraud Newsletter. The NHS Counter Fraud Authority (NHSCFA) estimates that the NHS is vulnerable to over £1.3 billion worth of fraud each year.

Fraud is deception carried out for personal gain, usually for money. Fraud can also involve the abuse of a position of trust. By 'NHS fraud' we mean any fraud where the NHS is the victim. While those who commit fraud against the NHS are a small minority, their actions have a serious impact on us all.

Fraud against the NHS could be committed by anyone. This includes members of staff, patients, contractors, suppliers, medical professionals and external parties, such as cybercriminals.

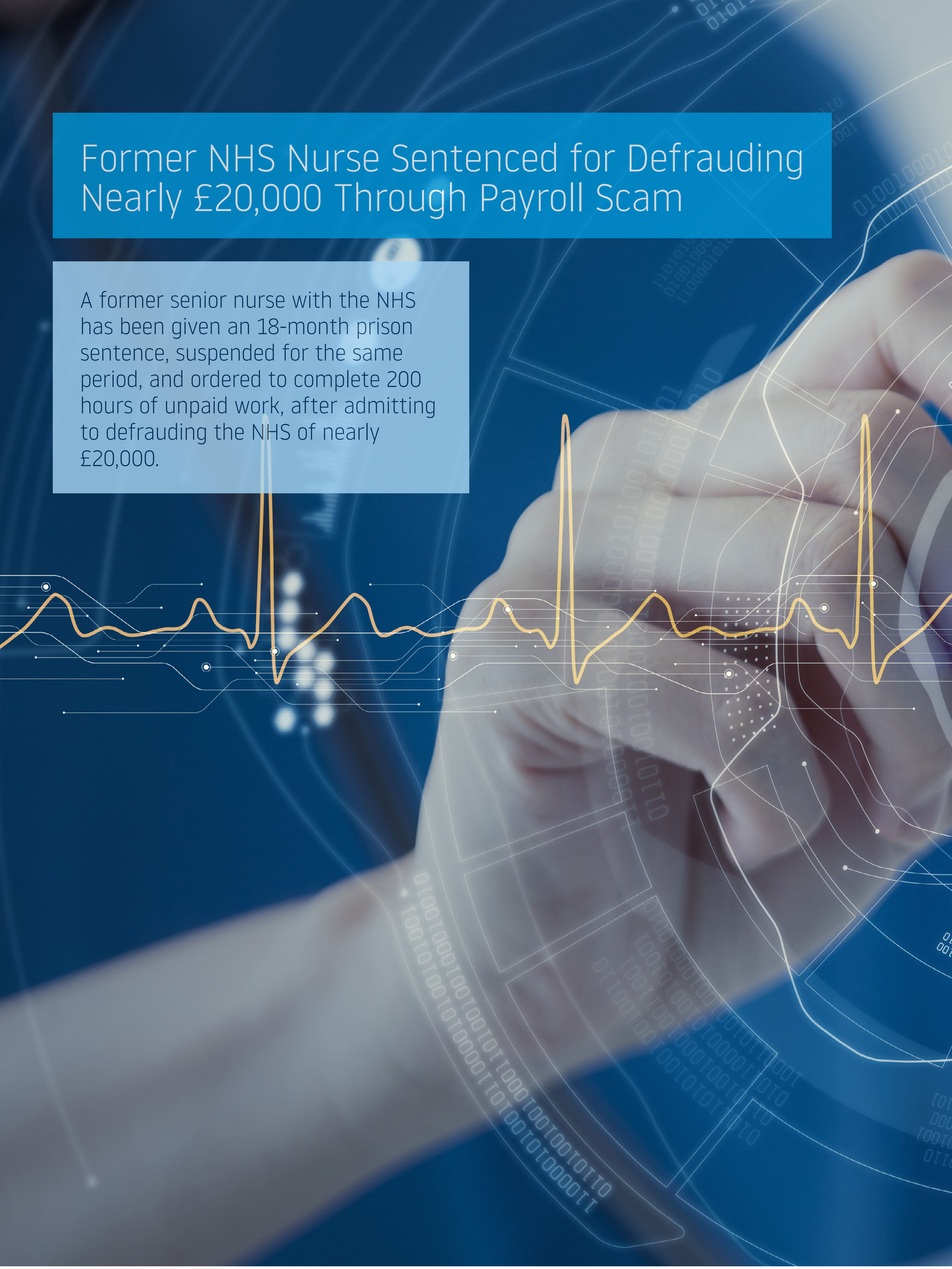
The Strategic Pillars

The NHSCFA 2023-2026 Strategy: 'Working together to understand, find and prevent fraud, bribery and corruption in the NHS' focuses on four key pillars: Understand, Prevent, Respond and Assure.

- **Understand** how fraud, bribery and corruption affects the NHS.
- We will ensure the NHS is equipped to take proactive action to **prevent** future losses from occurring.
- When we know that fraud has occurred, we are equipped to **respond**.
- We can **assure** our key partners, stakeholders and the public that the overall response to fraud across the NHS is robust.

Fraud takes taxpayers' money away from patient care and into the hands of criminals. Everyone has a part to play in fighting fraud and being aware of the risk and remaining vigilant are the most important first steps, followed by knowing how to report fraud.

Contact details for reporting fraud in confidence are included at the end of this newsletter so if you have any suspicions that fraudulent activity may be occurring, please report this at the earliest opportunity.



Former NHS Nurse Sentenced for Defrauding Nearly £20,000 Through Payroll Scam

A former senior nurse with the NHS has been given an 18-month prison sentence, suspended for the same period, and ordered to complete 200 hours of unpaid work, after admitting to defrauding the NHS of nearly £20,000.

The individual appeared at Reading Crown Court in April 2025, following a guilty plea to fraud by false representation under Section 2 of the Fraud Act 2006 at East Berkshire Magistrates' Court in September 2024.

They were suspended from their role as Senior Sister in the Emergency Department at the hospital at which they worked on 21 April 2023, after suspicions of fraudulent activity surfaced. An internal review revealed that between December 2020 and April 2023, they exploited their administrative privileges on the Trust's Health roster system to add shifts for themselves and claim payment for bank shifts they did not actually work, resulting in a loss of £19,575.41 to the Trust.

Having joined the Trust in January 2013, their seniority gave them the ability to manage and alter shift schedules, including their own, which they used to commit the fraud. In May 2023, they voluntarily attended an interview under caution and confessed to the fraudulent activity.

Their sentencing at Reading Crown Court included an 18-month suspended sentence, 200 hours of community service, and a requirement to complete 15 rehabilitation days. The NHS Counter Fraud Authority is now pursuing recovery of the stolen funds under the Proceeds of Crime Act 2002.

The Local Counter Fraud Specialist who led the investigation, commented that the individual had betrayed the trust of both their employer and colleagues, claiming pay for hours they did not work and forcing others to cover their absence. It is hoped that this case will deter others from defrauding the NHS.

The Chief People Officer at the NHS Foundation Trust reaffirmed the organisation's commitment to addressing fraud and encouraged staff to report any concerns so they can be investigated with the help of Counter Fraud Specialists.

Patient Receives Police Caution for Submitting Over £2,300 in False NHS Travel Claims

A patient who submitted fake taxi receipts and fraudulent travel claims totalling more than £2,300 to a Hampshire NHS Trust has received a Formal Police Conditional Caution following an investigation by the Local Counter Fraud Specialist (LCFS).

While some patients are legitimately entitled to claim help with travel costs for NHS appointments in England, this individual exploited the system by forging receipts and making false claims. After suspicions were raised, the LCFS worked with the Trust's Cashier's Officer and a local taxi company to gather evidence. Their enquiries revealed that the patient had claimed for 71 journeys that never took place and inflated fares on a further 15 occasions using counterfeit receipts, resulting in a total loss of £2,317.40 to the Trust.

The patient was interviewed under caution at Newport Police Station by two fraud specialists from the Fraud and Security Management Service, where they admitted to knowingly committing the fraud.

In December 2024, the patient accepted a Formal Police Conditional Caution as an alternative to prosecution. The conditions require full repayment of the losses to the Trust and written apologies to both the Senior Cashier and the Chief Finance Officer. This caution will remain on the patient's police record and may be disclosed to future employers.

Surge in Social Media and Email Account Hacking Prompts Urgent Security Warnings

Reports of social media and email account hacking surged in 2024, with Action Fraud recording 35,434 cases - an increase from 22,530 in 2023. In response, Action Fraud and Meta have launched a campaign urging the public to strengthen their online security by enabling two-step verification (2SV) on all accounts, as nearly £1 million was lost to hackers last year.

The main motives behind these hacks include investment scams, ticket fraud, and outright theft of accounts. The Deputy Director of Action Fraud highlighted that hacking remains the most frequently reported cybercrime this year and stressed the importance of taking steps to secure online accounts. He advised users to enable 2SV, use strong and unique passwords, ideally made up of three random words, and never share passwords with anyone else.

Meta's Security Policy Director, noted that cybercriminals are constantly evolving their tactics. Meta is addressing these threats by encouraging two-factor authentication and introducing facial recognition to help users regain access to compromised accounts.

Common hacking methods include:

- On-platform chain hacking: Criminals take over an account and impersonate its owner, often tricking contacts into revealing authentication codes. Once in control, they use the account to promote fraudulent schemes, such as fake investment opportunities or ticket sales.

- Leaked passwords and phishing: Hackers exploit passwords exposed in data breaches or obtained through phishing attacks. Since many people reuse passwords across different accounts, a single breach can compromise multiple accounts.

To reduce the risk of falling victim to these attacks, experts recommend:

- Activating 2-step verification on all important accounts, especially email and social media, to add an extra layer of security.

- Creating strong, unique passwords for each account, using a combination of three unrelated words to make them memorable yet difficult to crack.

- Reporting suspicious emails by forwarding them to report@phishing.gov.uk and, if you lose money or share financial details, contacting your bank and reporting the incident to Action Fraud.

QR Code Scams on the Rise: How Subscription Traps Are Catching Out UK Consumers

QR code scams, often referred to as “quishing,” are becoming increasingly common, with many people discovering unexpected recurring charges from unfamiliar companies after scanning QR codes in everyday locations like restaurants, shops, bus stops, and car parks. These subscription traps are now among the most frequently reported scams, with victims often unaware of how their payment information was obtained.

Criminals exploit the popularity and convenience of QR codes, those black-and-white squares that link your phone to a website, by placing counterfeit codes over legitimate ones or embedding them in online ads and pop-ups. Recent warnings from police highlight a sharp increase in QR code fraud, especially in public spaces such as parking areas.

A common tactic involves scammers posing as reputable businesses or services. Victims have reported being charged up to £39.99 per month for subscriptions they never knowingly agreed to, often after scanning a QR code to download an app or access a service. In some cases, the process is so confusing that people don’t realise they’ve signed up for a paid subscription until the first large payment is taken from their account.

Scammers may also make it difficult to cancel these unwanted subscriptions, with confirmation emails lacking contact details or containing broken cancellation links. Online reviews for these brands are overwhelmingly negative, reflecting the frustration and financial loss experienced by many consumers.

How QR code subscription scams work

Fraudsters can tamper with legitimate QR codes by placing their own stickers on top of the real ones, especially in public places like parking meters and restaurants.

Scanning these fake codes can lead to phishing websites, misleading adverts, or even malware installations, particularly if third-party QR scanner apps are used instead of the built-in camera app on smartphones.

Victims may be tricked into providing personal or financial details, or inadvertently sign up for costly recurring subscriptions.

What to do if you're affected?

If you notice a recurring payment you didn't authorise, contact your card provider immediately to stop further charges. Banks can sometimes block future payments, though refunds for already taken funds may be harder to obtain if the transaction appears authorised.

If the company refuses to refund you, escalate the issue with your bank, and if necessary, take your complaint to the Financial Ombudsman Service.

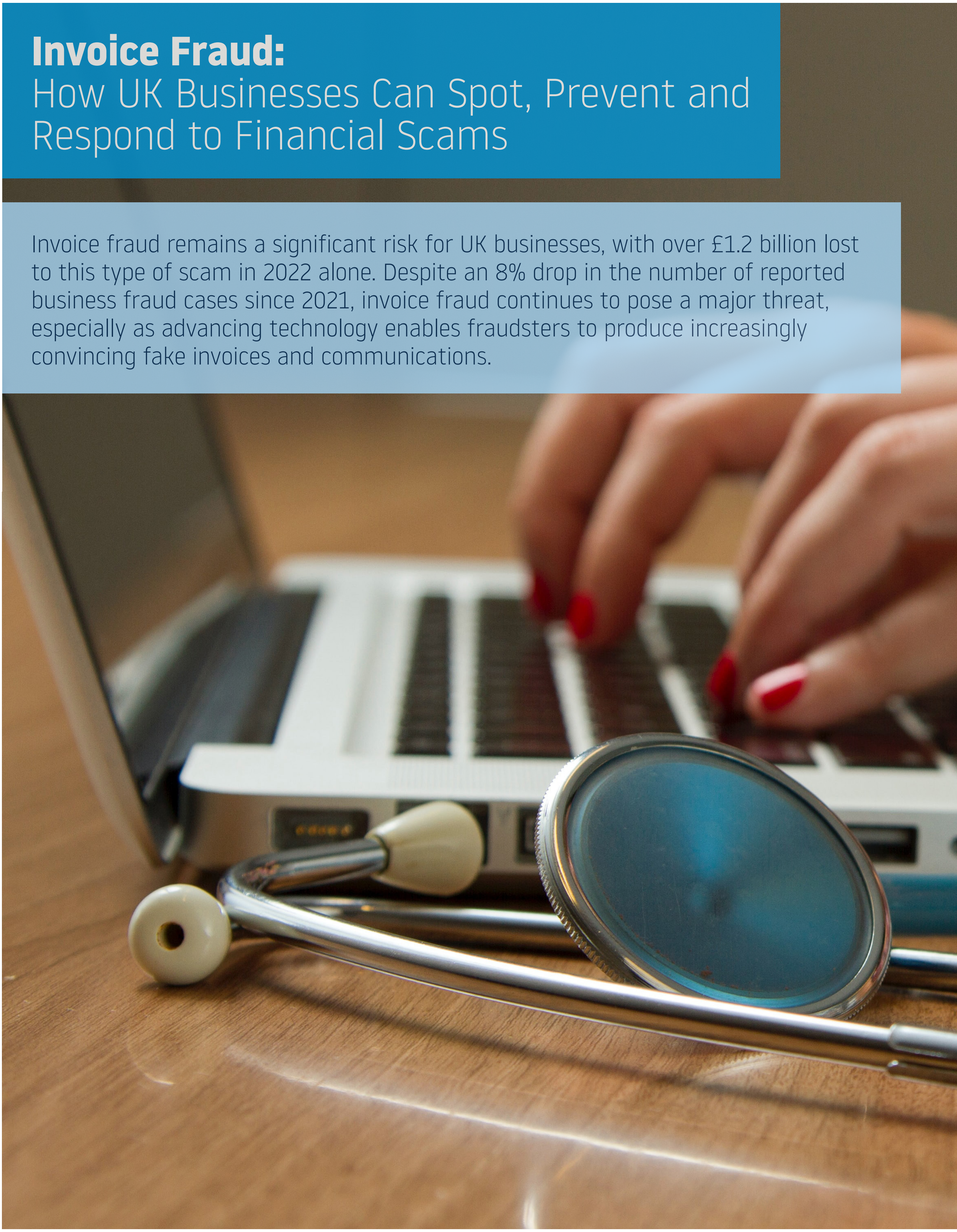
Tips for staying safe with QR codes

- Inspect QR codes for signs of tampering, such as stickers placed over existing codes, especially in public spaces. If unsure, manually type the web address instead of scanning.
- Use your phone's built-in camera to scan QR codes, not third-party scanner apps, to reduce the risk of malware.
- Preview the destination link before opening it. If the web address looks suspicious or doesn't match the expected site, don't proceed.
- Never use QR codes to download apps; always use official app stores.
- Be wary of QR codes in emails, as scammers increasingly use them to bypass email security and hide malicious links.

By following these precautions, you can reduce your risk of falling victim to QR code subscription scams. If you do spot an unauthorised payment, act quickly to limit further losses and seek help from your bank or the relevant authorities.

Invoice Fraud: How UK Businesses Can Spot, Prevent and Respond to Financial Scams

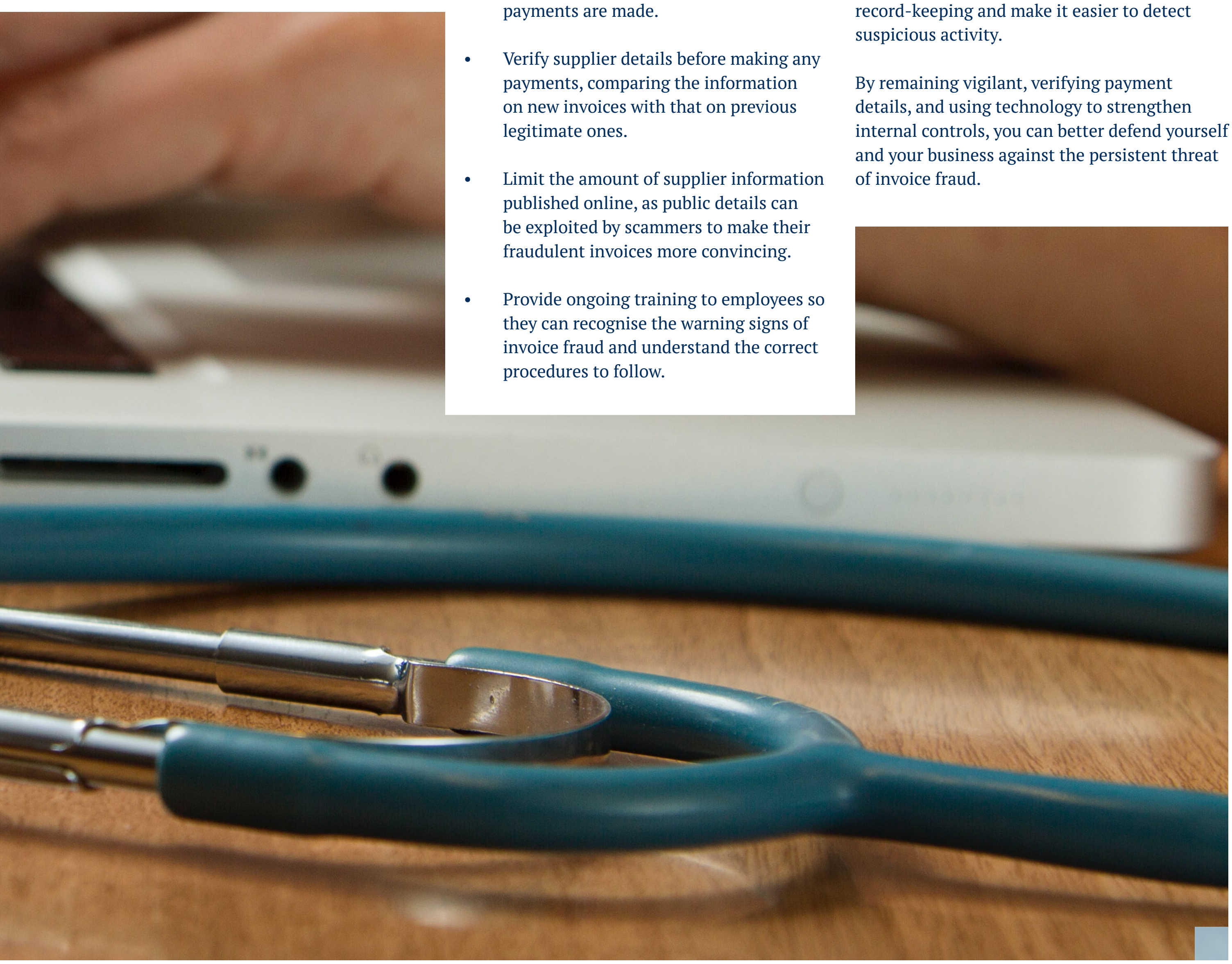
Invoice fraud remains a significant risk for UK businesses, with over £1.2 billion lost to this type of scam in 2022 alone. Despite an 8% drop in the number of reported business fraud cases since 2021, invoice fraud continues to pose a major threat, especially as advancing technology enables fraudsters to produce increasingly convincing fake invoices and communications.



Within Essex, detectives are looking into reports that GP surgeries and other organisations have received fraudulent invoices for office supplies, resulting in financial losses currently estimated in the tens of thousands of pounds. So far, five individuals have been arrested and interviewed on suspicion of fraud in connection with the case. All five have been released on bail with conditions as the investigation continues.

What is invoice fraud?

Invoice fraud occurs when criminals trick a business into transferring money to a fraudulent bank account, often by sending a fake invoice that appears to come from a trusted supplier or service provider. Scammers may impersonate existing business partners or hack into legitimate company emails, altering payment details on genuine invoices so that funds are redirected to their own accounts.



How to guard against invoice fraud

- Treat any email or message requesting a change in payment details with suspicion. Always verify such requests by contacting the supplier directly using established contact information, not the details provided in the suspicious message.
- Be cautious if you are pressured to make immediate payments or if the invoice lacks clear payment terms—these are common tactics used by fraudsters to rush decisions.
- Regularly reconcile invoices against your own records and confirm that you are being billed for goods or services you have actually received.
- Implement a robust payment approval process involving multiple staff members, such as finance and procurement teams, to cross-check and validate invoices before payments are made.
- Verify supplier details before making any payments, comparing the information on new invoices with that on previous legitimate ones.
- Limit the amount of supplier information published online, as public details can be exploited by scammers to make their fraudulent invoices more convincing.
- Provide ongoing training to employees so they can recognise the warning signs of invoice fraud and understand the correct procedures to follow.

What to do if you fall victim to invoice fraud

- Act swiftly. The sooner you respond, the greater the chance of recovering lost funds.
- Immediately contact your bank to report the fraudulent payment—this may allow them to freeze or reverse the transaction and block further payments to the scammer.
- Report the incident to authorities such as Action Fraud, and gather all relevant evidence, including the fraudulent invoice, correspondence, and payment records, to support the investigation.

Utilising technology for protection

Adopting digital invoicing and automated invoice-matching systems can significantly reduce the risk of invoice fraud by flagging discrepancies and ensuring only verified suppliers are paid. These tools also streamline record-keeping and make it easier to detect suspicious activity.

By remaining vigilant, verifying payment details, and using technology to strengthen internal controls, you can better defend yourself and your business against the persistent threat of invoice fraud.

Reporting Fraud

Everyone has a part to play in fighting fraud.

If you work for the NHS and suspect any fraud, bribery, or corruption against the NHS, please contact your Local Counter Fraud Specialist.

Alternatively, please contact the NHSCFA 24-hour reporting line by calling **0800 028 4060**, or by completing the online reporting form.

All reports are treated in confidence, and you have the option to remain anonymous.

In 2024, Scrutton Bland became part of Sumer – a collaboration of the best regional accountancy practices with a shared vision to champion local small to medium-sized enterprises. By bringing together the best in business services, Sumer retains the value that community-based practices offer and combines this with the scale, breadth of expertise and technologies that only a national organisation can muster.

To find out more about Sumer, visit our website: www.sumer.co.uk

0330 058 6559
scruttonbland.co.uk

@scruttonbland

0568/05/2025/MKTG

scruttonbland
Part of the SUMER Group