FRAUDULENT TIMES

April 2026

WELCOME TO THE LATEST EDITION OF FRAUDULENT TIMES

"This newsletter has been designed to highlight areas of fraud within the NHS and to help you understand why we need to combat it effectively. By raising awareness of fraud cases, it will help you to identify what fraud is and where it is most likely to occur. As always, I hope that you will find our newsletter a useful and interesting read. We value feedback on the content so if you have any comments or suggestions for topics in future editions, please email these to us at the address at the bottom of the page."

Craig Bevan-Davies
Assistant Director of Anti-Crime Services

TOP NEWS

Custodial sentence for former NHS credit controller in 300k fraud case

An NHSCFA investigation has led to the jailing of a former NHS credit controller after he and four co-defendants defrauded the NHS out of more than £300,000. The suspect was sentenced to three years and eight months' imprisonment.

Three-year prison sentence for former NHS resident doctor in £268k NHS fraud

A former NHS resident doctor has been sentenced to three years' imprisonment after pleading guilty to defrauding the NHS out of more than £268,000.
The suspect had been employed as a Trust grade specialist registrar - he worked on-call and night shifts at three additional trusts, despite informing his employer that he was unfit to do the same work for them.

Sentencing of former GP practice manager for £144k fraud

An investigation has resulted in a former NHS GP practice manager receiving a suspended jail sentence after pleading guilty to defrauding the NHS of more than £144,000. The suspect was sentenced to two years imprisonment, suspended for 18 months as well as 20 hours of rehabilitation and will be electronically tagged for four months.

360assurance.counterfraud@nhs.net

FRAUDULENT TIMES

April 2026

NHSCFA INVESTIGATION LEADS TO JAILING OF FORMER NHS MANAGER AFTER £123,000 NHS FRAUD

A joint investigation between 360 Assurance and the NHS Counter Fraud Authority (NHSCFA) has led to the jailing of a former NHS senior manager after he and two others defrauded the NHS of more than £100,000.

The suspect was employed by a Trust as a senior manager responsible for the management of Additional Roles Reimbursement Scheme (ARRS) staff in the Primary Care Networks. He used his position to set up a friend and a family member, who were not employees at the Trust, as 'ghost' contractors, with one claiming to be a physician associate and the other an advanced paramedic.

The suspect paid a total of £123,000 into their accounts between August 2022 and May 2023. Their crimes were exposed when an audit check showed that neither acquaintance were registered to the organisations named on their invoices.
The suspect was sentenced to two years and six months' imprisonment at Wolverhampton Crown Court on 16 January 2026. He had pleaded guilty to fraud by abuse of position, contrary to the Fraud Act 2006, at Dudley Magistrates' Court on 22 April 2025.

Paul Westwood, Counter Fraud Specialist at 360 Assurance said: "The outcome of this case demonstrates the NHS's robust and objective approach, and endeavour to ensure that anyone who attempts to defraud the NHS is brought to justice."

"This was a calculated scheme that diverted significant public funds away from frontline patient care. It was a deliberate abuse of position, with Gandy exploiting his senior role to manipulate NHS payment systems for his own personal gain. A Proceeds of Crime Act case will now begin to recover some of Gandy's illicitly obtained assets during his period of criminal activity. "

"The NHS is firmly committed to working tirelessly to protect vital NHS resources and we will continue to pursue those who seek to defraud our health service. "We encourage anyone with suspicions of fraud against the NHS to report it through our confidential reporting channels."

SYSTEM UPDATES!

ACTION FRAUD IS NOW KNOWN AS REPORT FRAUD.

Report Fraud is the new system for reporting to cybercrime and fraud to the police.

This service is run by the City of London Police, when you make a report of fraud you will receive a police crime reference number. Reports taken are passed to The Report Fraud Analysis Services team. The Report Fraud Analysis services team are responsible for the assessment of reports made and to ensure that reports of Fraud reach the right place.

Report Fraud is here to make you aware of the tactics and risks to help protect everyone within the cyberspace. Criminals operate everywhere online, including websites, apps, emails, text and phone, so it is essential to learn and understand what you can do to prevent the risks of fraud for yourself and to make others aware.

You can report cybercrime or fraud using the online reporting hub any time of the day or night, or by calling the cybercrime and fraud specialists by calling 0300 123 2040.

https://www.reportfraud.police.uk/

Report Fraud

https://www.360assurance.co.uk/

FRAUDULENT TIMES

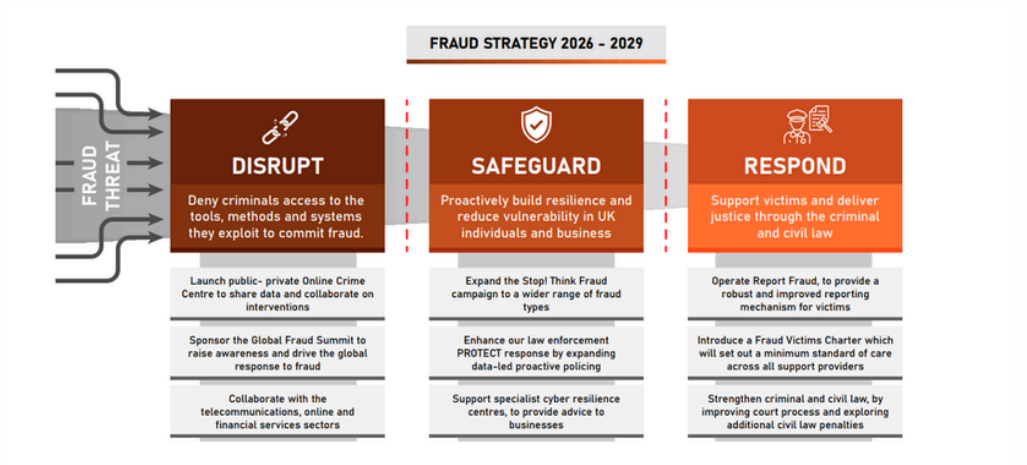
April 2026

THE FRAUD STRATEGY 2026 TO 2029

Fraud against individuals and businesses is evolving rapidly and causing significant harm, devastating its victims, eroding public trust and continues to pose a serious threats to the United Kingdom's national and economic security.

The Government will invest over £250 million between 2026 and 2029 to deliver this Strategy, aimed at combatting fraud against individuals and businesses.

This strategy introduces a new system-wide approach recognising the agility of criminals and the need for wide raging intervention. This approach is in three parts: **DISRUPT**, **SAFEGUARD** and **RESPOND**.



READ THE FULL FRAUD STRATEGY HERE:
CP 1523 – Fraud Strategy 2026-2029 Disrupting crime, supporting economic resilience and delivering justice

https://www.360assurance.co.uk/

FRAUDULENT TIMES

April 2026

PROTECT AGAINST FRAUD

Fraud remains a significant problem for the UK and remains the most prevalent crime against individuals in England and Wales, accounting for an estimated 41% of all crime reflected in the Crime Survey for England and Wales in the year ending September 2024.

National Campaigns Against Fraud have been launched through partnerships between the UK Government, National Cyber Security Centre and National Crime Agency – these joint campaigns are aimed at accounts payable professionals and finance personnel that highlights the risks of Frauds such as Invoice Fraud and Payment Diversion Fraud, costs businesses millions each year.

Figures released by Action Fraud revealed that in September 2025 alone, Invoice Fraud victims lost a total of £3,908,086 from 83 Report Fraud cases, averaging more than £47,000 per case. Invoice Fraud accounted for 85% of all Payment Diversion Fraud losses in September 2025.

These campaigns provide individuals and businesses with practical guidance on identifying and preventing these frauds including:

- **CHECK** for any changes to invoice details, bank details or if you are being pressed for an urgent payment.
- **VERIFY** by calling the genuine supplier on a previously used phone number before you transfer money, as emails can be intercepted or diverted.
- **NEVER** transfer money until you are satisfied the details are correct.

Protect yourself by securing your accounts, data and devices

- Use a strong and different password for your email using 3 random words. Your email password should be strong and different from all your other passwords.
- Always use 2-step verification (2SV), where available, to protect your email account.
- Use your browser's password manager to safely store your passwords.

Recognise and break suspicious contacts

- If you have any doubts about a message or phone call, contact the organisation directly to check. Use contact details from their official website – don't use the numbers or address in the message.

NATIONAL CAMPAIGNS

"FRAUDSTERS AREN'T FUSSY. THEY'LL PICK ON ANYONE"

Nobody is immune from fraud. The criminals behind it target people online and in their homes, often emotionally manipulating their victims before they steal money or personal data.

By staying vigilant and always taking a moment to stop, think and check whenever we're approached, we can help to protect ourselves and each other from fraud.

STOP! THINK FRAUD

Fraud accounts for almost 41% of all crime. In just one year, 1 in 16 adults in England and Wales were victims of fraud.

That's nearly 3 million of us.

1 in 5 businesses were also a victim of fraud over a 3-year period.

In other words, fraud is rife, and it can happen to anyone.

Source: Crime Survey for England and Wales, year ending June 2024

Source: Economic Crime Survey 2020

https://www.360assurance.co.uk/

NCA National Crime Agency

In partnership with NatWest

STOP! THINK FRAUD

INVOICE FRAUD

Invoice Fraud is one of the most common and costly forms of financial crime affecting individuals, families and businesses.

Invoice Fraud happens when criminals deceive you into paying a fake invoice or diverting a genuine payment into their own bank account. Fraudsters can impersonate suppliers, intercept emails or send convincing invoices to generate immediate payments into their own accounts

Knowledge of Invoice Fraud is the best protection.

CHECK

for any changes to invoice details, bank details or if you are being pressed for an urgent payment.

VERIFY

by calling the genuine supplier on a previously used phone number before you transfer money, as emails can be intercepted or diverted.

NEVER transfer money until you are satisfied all details are correct.

Invoice Fraud is a sign of the sophisticated tactics of criminals, not a sign of your negligence. Knowledge, verification, and robust processes are the most proven effective safeguards.

PROTECT YOUR BUSINESS

Fraudsters will use urgency and communicate with authority and knowledge of your business. They will attempt to impersonate your supplier in order to gain your money.

Be vigilant of the warning signs:

- Communication claiming to be 'urgent' or claiming 'late payments'
- Messages stating a regular supplier's bank details have changed
- Invoice details that do not match previous genuine invoices, such as amounts, reference numbers or contact names
- Look out for minor changes to your suppliers email address
- Unexpected invoices or payment demands for goods or services you do not recognise
- Unusual language, grammar and spelling to those of your regular supplier

DO NOT FEEL PRESSURED INTO MAKING A PAYMENT
IF YOU ARE UNSURE OR HAVE CONCERNS

PROTECT YOUR ACCOUNTS

- Always confirm bank detail changes using a published phone number or long standing contact that you have used before
- Consult another colleague to authorise high value payments
- Cross check any new invoices with a previous genuine example
- Educate yourself and your teams on fraud risks to ensure they are aware of the warning signs

VULNERABLE IT SYSTEMS CAN BE HACKED
Ensure computer IT systems are secure, passwords changed regularly and anti-virus software is up to date

IF YOU SUSPECT YOU HAVE BEEN A VICTIM OF INVOICE FRAUD OR AN ATTEMPT, IMMEDIATELY CONTACT :

1. **YourBank**
   Ask them to freeze the funds and account whilst investigation takes place.
2. **Report Fraud**
   Submit a report online or by calling 0300 123 2040.
3. Retain all emails, invoices and communication trails to support the investigation.

NCA National Crime Agency | The Law Society | Solicitors Regulation Authority | STOP! THINK FRAUD

PAYMENT DIVERSION FRAUD

Criminals are actively targeting property purchases, with the aim of tricking you into transferring your client's property price to them.

The criminals can pretend to be another lawyer or a bank in order to con you into sending your client's payment to the wrong account.

CHECK

by calling before you transfer money, as emails can be intercepted or diverted.

TEST

the account is genuine by sending a small sum to the account details provided and ensure it has been received correctly.

NEVER transfer money until you are satisfied the details are correct.

No one should lose an entire deposit or the full property purchase funds from your firm because of **Payment Diversion Fraud (PDF)**.

PROTECT YOURSELF

Get bank details directly from the law firm in person or on the phone at the start of the conveyancing process.

If you receive an email or call stating a change in bank details, question it's authenticity.

LAW FIRMS RARELY CHANGE THEIR BANK DETAILS

Always check the bank details directly with YOUR solicitor.

If you have doubts check with a senior person at the firm by calling them on their published number, not the one given in the email demanding payment. If you cannot speak to your lawyer, contact someone senior or a staff member you have spoken to before. You can ask them to confirm the details by post.

Do not feel pressured into changing any details before you have spoken to someone senior from the firm.

PROTECT YOUR CLIENTS

Inform your clients to check bank details are correct directly with you before sending any funds.

Ensure clients set strong and separate passwords for your accounts, and ensure antivirus software on your devices; these frauds often rely on compromised accounts.

Ask your vendor/purchaser not to use public or unprotected Wi-Fi systems to check emails during the conveyancing process.

VULNERABLE WI-FI CAN BE EASILY HACKED

Advise clients to avoid posting on social media about buying or selling a property or securing a mortgage. Fraudsters may target them because of this.

IF YOU SUSPECT YOU HAVE BEEN A VICTIM OF PDF IMMEDIATELY CONTACT :

1. **YourBank**
   Ask them to contact the receiving bank to freeze the funds.
2. **Action Fraud**
   Submit a report online or by calling 0300 123 2040.
3. **YourSolicitor**
   They may be being targeted and other clients may be **at risk.**

FRAUDULENT TIMES

April 2026

SECURITY MANAGEMENT SERVICES (SMS)

Security management is the identification of an organisation's assets including people, buildings, machines, systems and information assets, followed by the development, documentation and implementation of policies and procedures protecting these assets.

We work in conjunction with your organisation to protect patients, staff & NHS property, with the purpose to provide a safe and secure environment for all, so that the highest level of clinical care is provided.

The role of the LSMS is to create and promote a pro-security culture within the organisation. This includes the following:

- To investigate security incidents/breaches in a fair, objective and professional manner so that the appropriate sanctions are taken and consideration of preventative action takes place.
- Support the organisation with compliance against the Violence Prevention and Reduction Standards.
- Working with the Organisation to undertake site-based security visits in relation physical security, access controls. Covering buildings, assets of the Organisation to ensure appropriate processes.

CASE STUDY

Following an assault on a board member at an NHS organisation, our LSMS carried out an investigation into the incident which resulted in a civil injunction being placed on the individual. The injunction included banning the individual from visiting any location belonging to the organisation and any location where the board member would be attending public meetings. The individual was further prosecuted by the police for physical assault.
The individual will also receive regular warning letters in relation to their behaviour when contacting staff to ensure they are aware of the appropriate and acceptable behaviour. The letter informs the individual that behaviours displaying verbal aggression, threatening behaviour is unacceptable and will not be tolerated.

OUR SMS SERVICES

- **Crime reduction and security surveys of premises providing detailed risk assessment and practical, cost-effective, recommendations**
- **Comprehensive investigation of all types of security incidents**
- **Liaison with the police, local authorities and other regulatory bodies**
- **Advice to management and staff on general or specific security issues**
- **Comprehensive local security management services, including annual work plans, progress and annual reports, and annual data returns**
- **Audit of provider security contract delivery to ensure that regulatory and licensing requirements are met**
- **Provision of comprehensive security and conflict resolution training delivered by accredited trainers**

CONTACT

Shaun Grayson
Security Management Specialist
Email: shaun.grayson1@nhs.net

FRAUDULENT TIMES

April 2026

MEET THE COUNTER FRAUD TEAM (LOCAL COUNTER FRAUD SPECIALISTS)

Craig Bevan-Davies
Assistant Director of Anti - Crime
craig.bevan-davies@nhs.net
Mob: 07785 445905

Claire Croft
Principal Anti-Crime Specialist
claire.croft1@nhs.net
Mob: 07920 138354

Joanna Clarke
Principal Anti-Crime Specialist
joanna.clarke3@nhs.net
Mob: 07816 272666

Matt Treharne - Clarke
Principal Anti-Crime Specialist
matt.treharne-clarke@nhs.net
Mob: 07990 084824

Daniel Mason
Principal Anti-Crime Specialist
daniel.mason15@nhs.net
Mob: 07464 521746

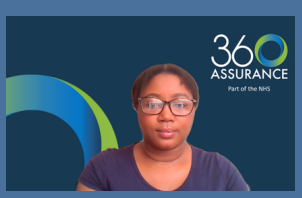
Michelle Dixon
Principal Anti-Crime Specialist
michelle.dixon3@nhs.net
Mob: 07557 316156

Paul Westwood
Principal Anti-Crime Specialist
pwestwood@nhs.net
Mob: 07545 502400

Dipixa Bhundia
Counter Fraud Specialist
dipixa.bhundia@nhs.net
Mob: 07824 499371

Chris Taylor
Counter Fraud Specialist
christaylor2@nhs.net
Mob: 07342 072907

Ian Morris
Counter Fraud Specialist
ian.morris7@nhs.net
Mob: 07920 138606



Sophia Umoh
Counter Fraud Specialist
sophia.umoh@nhs.net
Mob: 07920 814338

Samantha Pacey
Counter Fraud Specialist
samantha.pacey1@nhs.net
Mob: 07920 138323

FRAUDULENT TIMES

April 2026

SCAN THE QR CODE TO REPORT ANY SUSPICIOUS FRAUD, BRIBERY OR CORRUPTION.

*"Working together to **find**, **report** and **stop** NHS fraud"*

NHS Counter Fraud Authority

For more information about fraud against the NHS, please visit the NHSCFA's website.

If you have **any** suspicions or concerns about fraud in the NHS you can:

- Talk to your Counter Fraud Champion or Counter Fraud Specialist
- Report them direct to the NHSCFA https://cfa.nhs.uk/report-fraud
- By calling **0800 028 4060** (available 24 hours).