



CASES IN COURT
Real Life Cases

→ SEE PAGE 2



FRAUD PREVENTION
Advice

→ SEE PAGE 4



NEWS
Fraud news to note

→ SEE PAGE 6

Introduction

The National Crime Agency website states that fraud remains the most common crime type experienced by victims in England and Wales. Fraud costs the UK many billions of pounds every year. The impact of fraud and related offences can be devastating, ranging from unaffordable personal losses suffered by vulnerable victims to impacting the ability of organisations to stay in business.

Everyone has a part to play in fighting fraud. Being aware of the risk and remaining vigilant are important first steps, followed by knowing how to report fraud.

This latest edition of Fraud Stop covers cases in court, fraud prevention advice and news on other targeted action being taken to prevent fraud in the UK.



CASE STUDY:

Social club employee convicted of multiple frauds and theft

Sussex Police report that a former employee who abused her position at a not-for-profit social club to steal thousands of pounds has been convicted at court.

The fraudster was an administrator for Hailsham Memorial Institute (HMI) – a club established in 1920 in memory of a local soldier who lost his life during the First World War.

She was appointed the paid role of administrator in 2006 and engineered absolute financial control of the club. However in 2019, club members became concerned about her actions when they failed to receive confirmation of receipt of funds raised at a charity event held by HMI in aid of Orchid Cancer Charity.

After an internal investigation conducted by HMI, the fraudster was dismissed from her role in August 2019. The matter was then reported to Sussex Police and a three-year investigation commenced which uncovered large scale frauds, thefts, and abuse of position offences.

The investigation found that she had stolen from HMI and made fraudulent claims against the club. These included falsifying her employment contracts to pay herself a higher salary, giving herself pay rises without authorisation, withholding payments to HMRC, false accounting, and laundering £26,000 of the stolen money out of the country to India.

Furthermore she falsified weekly accounts to steal cash from the social club and would often include personal purchases in receipts claimed back from the club. Payments were also received into her bank account for events and services provided by HMI and she failed to pass on money raised at HMI fundraising events to charities, including approximately £3,000 to the male cancer charity Orchid.

When asked to account for the money that was raised, the fraudster insisted she'd made the payment but could not find the receipts to prove it. When confronted by the members she tried to falsify the receipts and staged a fake discovery of the "lost" cash to cover her tracks.

During the investigation, the fraudster also made fraudulent claims for Universal Credit which were uncovered by police.

The investigation resulted in her being charged with 11 offences. Her trial began on 18 September 2023 at Hove Crown Court. During trial, she pleaded guilty to fraud by abuse of position but maintained her innocence in relation to all the other charges.

On Friday 20 October 2023, she was found guilty of eight of the 11 charges against her – four counts of fraud by abuse of position; fraud by false representation; theft; transferring criminal property; and fraud by failing to disclose information.

The fraudster has been released on court bail ahead of sentencing on 1 December 2023.

CASE STUDY:**Woman stole £70K and sent it to friends and family**

Nottinghamshire Police report that a customer service advisor stole almost £70,000 from her employer and sent it to seven others in order to launder the proceeds from her crime.

The fraudster used her position at E.ON to facilitate a series of refunds that she paid to family members and friends who in return refunded some of the money to her.

Police launched an investigation after E.ON reported £69,844 had been issued as false refunds by her between October 2016 and March 2021.

The company told detectives it had uncovered evidence that the customer service advisor had abused her position in order to create the false refunds, which she passed onto friends and family in the form of cheques.

The police investigation found the fraudster had made changes to the E.ON systems in order to process the fraudulent refunds.

She attended a voluntary police interview in which she confessed to her offending, adding that she had “fully messed up”.

She admitted processing refunds totalling £69,844 and that the amount of money deposited back into her own account was approximately £24,000.

She was charged and put before Nottingham Crown Court, where she pleaded guilty to fraud by abuse of position and acquiring / using / possessing criminal property

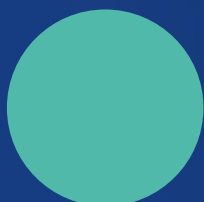
She appeared at the court on 26 October 2023 for sentencing and was jailed for two years, suspended for two years and appeared alongside her seven co-defendants, who each pleaded guilty to acquiring / using / possessing criminal property. Five out of the seven received suspended prison sentences, one was given a community order and one was discharged conditionally.

Council workers jailed for £1.5million lift repairs fraud

Two council workers from a borough in London have been jailed for their part in a £1.5m fraud involving unnecessary lift repairs.

At the end of March 2023 both were found guilty of conspiracy to commit fraud by abuse of position at Woolwich Crown Court and sentenced to five years and three-and-a-half years respectively.

The pair defrauded taxpayers in the Royal Borough of Greenwich of just over £1.5m by raising unnecessary lift repairs that were completed by an external contractor who invoiced the council for the repairs. The contractor then made personal payments to the pair as a reward for raising the unnecessary repairs.



Former solicitor jailed for defrauding clients of almost £2million

The Crown Prosecution Service (CPS) report that a former solicitor who defrauded clients at his firm of almost £2 million has been jailed.

On 22 September 2023, the fraudster was sentenced to four years imprisonment at Norwich Crown Court for committing fraud by abuse of position over almost a two-year period.

At the time of his offending, he was a senior partner at the firm he worked for, and his professional responsibilities included looking after client money and estates. In April 2015 he was led to believe he had won a postcode lottery in Spain and that in order to release the funds promised to him, he would need to make ever increasing demands for payments. This was a scam.

After exhausting his and his wife's money to make payments to the lottery scheme, the fraudster began taking money from the accounts of clients at his firm.

Between 21 August 2015 and 26 July 2017, he was responsible for making 72 transactions out of client accounts, worth a total value of £1,963,659.44. This affected 29 client accounts, six payments were also made from investment portfolios held by Trusts in his control, and further payments made from personal bank accounts of clients where he had Lasting Power of Attorney.

When concerns were first raised by the firm, he lied and made numerous excuses about investing the clients' money elsewhere, before finally admitting he was using the money for a lottery scheme.

Following an investigation by Norfolk Police, the CPS authorised the charge against him which he pleaded guilty to.

Spotting the Red Flags

Here are just some of the top signs that indicate that a colleague may be engaging in fraud:

- they are the first person to arrive or the last person to leave and therefore have opportunities to work unsupervised
- having unexplained wealth, living beyond their apparent means or a sudden change in lifestyle may be a cause for concern
- skipping approval steps or an unwillingness to share duties
- being reluctant to take annual leave – fraudsters avoid holidays so that other people won't review their work
- being in frequent communication with external parties, telephone conversations, text messages, emails and so on while at work or on breaks
- showing stress without having a high workload or undergoing noticeable personality changes such as displaying anxiety in response to routine questions
- having close relationships with suppliers/ contractors or customers insisting on dealing with just the one individual
- gambling and addiction habits can result in fraud

Is your email password strong enough?

Advice from the National Cyber Security Centre is to use a strong and separate password for your email.

If you've used the same password across different accounts, cyber criminals only need one password to access all your accounts.

Always use a strong and separate password for your email - a password that you don't use for any of your other accounts.

If a criminal can access your email account, they could:

- access personal and financial information about you
- send emails and post messages pretending to be from you
- reset all your other account passwords and get access to all your other online accounts

NCSC advice is to combine three random words to create a password that's 'long enough and strong enough'.

Weak passwords can be cracked in seconds. The longer and more unusual your password is, the harder it is for a cyber-criminal to crack.

Avoid creating passwords from significant dates or from your favourite sports team, or by using family and pet names. Most of these details can be found within your social media profile.

If you're thinking of changing certain characters in your password (so swapping the letter 'o' with a zero, for example), you should know that cyber criminals know these tricks as well. So your password won't be significantly stronger, but it will be harder for you to remember!

National Fraud Initiative – does your organisation take part?

The National Fraud Initiative (NFI) is an exercise that matches electronic data within and between public and private sector bodies to prevent and detect fraud. Many of the risks addressed by NFI are relevant to organisations such as housing associations and academies, as well as the mandated organisations such as local authorities.

Click on the link for case studies that illustrate the type of frauds that the NFI can help organisations identify:

<https://www.gov.uk/government/publications/national-fraud-initiative-case-studies/nfi-public-sector-case-studies>



Failure to prevent Fraud offence

The government is creating a new failure to prevent fraud offence to hold organisations to account if they profit from fraud committed by their employees. This will improve fraud prevention and protect victims. The new offence will strengthen existing powers to fine and prosecute organisations and their employees for fraud.

Under the new offence, an organisation will be liable where a specified fraud offence is committed by an employee or agent, for the organisation's benefit, and the organisation did not have reasonable fraud prevention procedures in place. It does not need to be demonstrated that company bosses ordered or knew about the fraud. This will discourage organisations from turning a blind eye to fraud by employees which may benefit them and will encourage more companies to implement or improve prevention procedures.

However to ensure burdens on business are proportionate, only large organisations are in scope defined as organisations meeting two out of the three of the following criteria:

- More than 250 employees
- More than £36 million turnover
- More than £18 million in total assets

Whistleblowing

Almost daily in the media, there continues to be organisational scandals, all of which could have been mitigated had there been more effective Board oversight.

Whistleblowing or raising concerns to do with safety, financial impropriety, and environmental risk, benefit your organisation in the long-term. Raising concerns is the first step in tackling them.

Board members of public bodies and companies have responsibilities in law and obligations under codes of conduct. That means a decision not to investigate and respond appropriately may not prove to be in line with the law and codes of conduct.

- [Listen to our podcast](#) with David Foley and Professor Dave Lewis on the subject of Whistleblowing and Organisational Culture
- [View the recording](#) of our Whistleblowing and Organisational Culture webinar
- [Visit our website](#) for more information. Contact TIAA for independent assurance on how whistleblowing is managed at your organisation

Disclaimer:

The content of this document is intended to give general information only. Its contents should not, therefore, be regarded as constituting specific advice, and should not be relied on as such. No specific action should be taken without seeking appropriate professional advice.

For further discussion and support, or if you suspect any fraud, bribery or corruption against your organisation, contact you Anti-Crime Specialist or:

- **Nick MacBeath, Senior Governance Manager, Anti-Crime Services,**
Email: nick.macbeath@ttaa.co.uk
OR
- **Melanie Alflatt, Director - Risk and Advisory, Email: fraud@ttaa.co.uk**