tiaa

FRAUD STOP

Spring 2023

CASES IN COURT

Details of recent court cases

→ SEE PAGE 2

SCAM ALERTS

Current scams in circulation that can target anyone

→ SEE PAGE 3

FRAUD ALERTS

What other frauds are targeting organisations?

→ SEE PAGE 4

Introduction

The National Crime Agency website states that fraud is the most commonly experienced crime in the UK and costs the UK many billions of pounds every year. The impact of fraud can be devastating to individuals and organisations. Fraud is deception carried out for personal gain, usually money.

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 edition covers cases that have been in court recently, other common frauds targeting organisations, common scams in circulation and a checklist for preventing fraud.

University finance head jailed for six years

A University of Brighton employee who stole more than £2million in cash over 30 years was jailed in March 2023.
The fraudster appeared at Hove Crown Court on 16th March 2023, where he was sentenced to six years in jail having previously pleaded guilty to fraud by abuse of position, theft by an employee and false accounting.
He used his position as the Head of Income and Payments at the university to embezzle around £2.4million and cover up his activity through fraudulent entries in the university's accounts.
A confiscation order is also due to be determined based on his illicitly gained funds, although is it unlikely that the full amount will be recovered.

Primary school bursar jailed for six years

A woman has been found guilty of stealing almost £500,000 from the primary school where she worked.
She appeared at Kingston Crown Court in February 2023 charged with four counts of fraud.
The fraudster, who worked as the school business manager, used her position to transfer funds to herself and increase her own pay.
She also claimed to be working 30 hours per week at the school's breakfast and afterschool club.
The deception enabled her to fund an extravagant lifestyle, including luxury holidays and cars.
On 31st March 2023, she was jailed for six years. A proceeds of crime hearing is set to take place at a later date.

Jail for man who stole from cancer charity

A police investigation has ensured that a man who stole more than £100,000 of other people's charity donations has been jailed. The fraudster was jailed for 40 months in November 2022 at Crown Court, having previously pleaded guilty to the count of fraud by abuse of position. A Proceeds of Crime Act hearing will take place to establish whether any of the funds can be recovered.

The investigation found that over a period of several years, he defrauded the charity of more than £100,000 of donations, raised by volunteers through community activities.

When asked to account for the loss of donations, the fraudster submitted forged documents to the charity. During questioning by police officers, he defended his actions by saying that amounts may have been incorrect due to stress but he did admit to keeping some cash donations for himself to fund a lifestyle above his means.

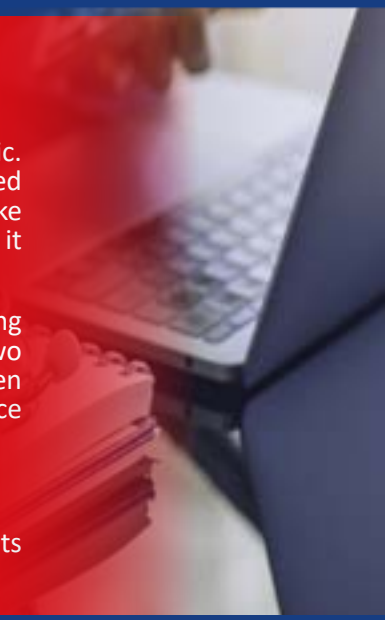
Overlapping Shifts

Staff working overlapping shifts has become increasingly more prevalent since the pandemic. Intelligence suggests that the increase in remote working can cause staff to become disconnected from their employer which subsequently increases the opportunity for staff to undertake overlapping employment. Whilst an employer may not object to staff working a second job, it should not conflict with their primary employment or adversely impact either employer.

TIAA has observed an increase in the number of referrals received where duplicate or overlapping employment is the key factor. A recent investigation concerned an individual who had two laptops for two separate Trusts, open on a desk at the same time. These matters have been difficult to prove to a criminal standard because of weaknesses in the organisation's governance and/or remote working procedures.

Action Point

Remedial recommendations are that the organisation provides clear guidance to staff on its expectations regarding secondary employment.



Scam alerts - Criminals are targeting WhatsApp users by posing as a friend and asking for a security code.

In a variance of a previous WhatsApp scam, Action Fraud is reporting 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 is a member of a WhatsApp group you are 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.

ADVICE FROM ACTION FRAUD IS TO:

- **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 is 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.**

Mandate fraud

Mandate fraud occurs when someone contacts an organisation with a request to change a direct debit, standing order or bank transfer mandate, by purporting to be from a genuine supplier that payments are made to. If the organisation accepts the fraudulent request, the payments are then diverted into the criminal's bank account.

Organisations are continuing to be victims of increasingly sophisticated mandate frauds. A TIAA client came very close to losing nearly 200K recently after fraudsters hacked into an email address of a Director of a supplier and communicated with the organisation's finance staff regarding a change of bank account and the provision of a phone number for the security checks to be completed. When the fraudsters realised that they would need supplier information for the security checks, they then created a fake organisation domain and communicated with the supplier for the requested information, purporting to be finance staff.

Action Point

Does your organisation receive assurance on IT security from suppliers when entering into contracts?

Contact your Anti-Crime Specialist for advice on mandate fraud prevention.

Fake positive covid test results

A TIAA Anti-Crime Specialist has conducted a number of investigations where staff have provided fake positive covid test results, leading to the staff being dismissed and salary repaid for false sickness absence. Here are just a couple of images of the 'positive' tests supplied to support time off sick.

There is no serial number on this test – it has been obtained from google images!

This image clearly has two drawn on lies purportedly showing a positive result!

Action Point

Line Managers should scrutinise images of test results and escalate any concerns.

Anti-Fraud Checklist

Does your organisation have an anti-fraud checklist? Remember fraud occurs in every sector. Consider the following:

- Are boards and key staff such as the chief financial officer aware of the risk of fraud and their responsibilities regarding fraud?
- Is fraud a regular item on the audit committee agenda?
- Does the risk management process include fraud risk?
- Does the organisation have a fraud strategy or policy, and is it promoted across the organisation?
- Does the organisation have policies on whistleblowing, declarations of interest and business conduct?
- Does the organisation have appropriate segregation of duties around financial transactions?
- Is it clear to whom suspicions of fraud and corruption should be reported?
- If there has been any fraud, has a 'lessons learned' exercise been completed?
- Is there robust system security in place to prevent cyber crime?

TIAA has developed a series of reviews that are designed to provide your organisation with assurance over key fraud risk areas. These include:

- A bespoke Fraud Risk Assessment which provides an assessment of the controls to mitigate against fraud
- Transactional Deep Dive review work using data analytics and data mining tools
- Fraud Preparedness – such as reviewing policies and fraud awareness training

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

- **Nick MacBeath, Senior Governance Manager, Anti-Crime Services ,** nick.macbeath@tiaa.co.uk
- **Or Melanie Alflatt, Director – Risk & Advisory,** fraud@tiaa.co.uk