SUMMER 2021

FRAUD STOP

tiaa

Fraud Triangle

Rationalisation, Opportunity and Incentive

Investigation Case Studies

Cases in Court

Cyber Fraud and Risks

Latest News

www.tiaa.co.uk

FRAUD SMART

The Perfect Storm for Fraudsters

The extended period of major business disruption arising due to the COVID pandemic has created unique opportunities for fraudsters, either by employees or third parties. A reflection on the impact that the disruption has had on the three elements required for a fraud to occur is testament to this.

Rationalisation: Many peoples' lives will have been significantly impacted by the pandemic and this may include: loss of financial well-being (either directly or by others in their family group); seeing others do well during the pandemic; and why plan for the long-term syndrome. The numbers impacted are unprecedented in recent history and will range across the full spectrum of the population.

Opportunity: There have been so many changes made to business systems in reaction to the pandemic, rather than through extensive pre-planning. Internal control would not have been the first consideration for many and indeed there was pressure to make things happen to keep the economy going. There has never been such a hiatus in terms of disruption of long established internal controls and checks.

Incentive: With the almost overnight move to remote working and digitalisation combined with an 'others have benefited from the COVID disruption' factor it is likely that the threshold for people to be tempted to commit fraud has never been so low.

We therefore suggest that the key first stage for organisations is to instil the message, backed up by proactive action, that they are committed to rooting out persons endeavouring to take advantage of the business disruption and that fraud still does not pay.

The court system is only just recovering and as a consequence it is far too early for any trends to be identified. The cases referred to in this Fraud Stop have therefore been selected as examples of clear and present fraud risks which could be currently being perpetrated at Councils.

Taking Advantage of a Salary Sacrifice Scheme

A finance administrator stole £6,000 of vouchers from the Council at which they were employed. They were sentenced to a community order.

The finance administrator's role included approving cycle to work applications made by their colleagues. These were through a salary sacrifice scheme and their role included setting up the salary sacrifice payments with payroll.

The finance administrator approved £6,000-worth of vouchers for themself to use, but did not set up salary sacrifice payments.

The finance administrator redeemed the vouchers at Halfords and bought numerous bikes, before selling them on Facebook for £500 each. In one Facebook post, they wrote: 'Fully legit, just using a voucher from the cycle to work scheme.'

It was not disclosed how the fraud was detected, but it is noted that this person changed roles within the Council and the frauds were committed whilst in their new role.

COVID Lessons: Many organisations have introduced and or extended salary sacrifice schemes for staff. This has included furniture and other equipment for working from home. Regular reconciliations of expenditure against committed recovery amounts on payroll need to be in place.

Taking Advantage of Business Rate Refunds

A business rates officer fraudulently transferred £80,000 of business rate refunds to their friends over an eighteen month period. They were sentenced to eighteen months' imprisonment.

The business rates officer applied a period of empty property relief totalling £4,000 on a named company, despite records showing the company had been dissolved. They created a new bank account and creditor address associated with the business that in fact belonged to their co-conspirators.

The fraud was identified when another member of staff looked into this business rates refund by chance. When confronted they initially claimed they were correcting an existing error. An internal investigation was launched and it was found that the business rates officer had altered banking information and addresses of other businesses to make a total of 26 separate fraudulent transfers.

COVID Lessons: The number of businesses which may cease to trade as a result of the business disruption is likely to significantly increase. Furthermore, there could be a temptation for businesses to incorrectly state their premises have been empty during the pandemic. A check of organisations claiming empty property relief against those provided with emergency grants may identify possible inconsistencies.

Taking Advantage of the Online Market to Sell Council Assets

An electrical contracts supervisor fraudulently sold £10,000 of council equipment over a four year period. They were sentenced to an eight month curfew order.

The supervisor stole 200 separate items including heat and smoke alarms and other equipment and sold them on eBay.

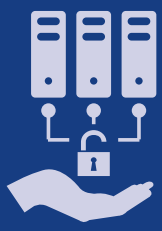
The fraud was identified after another user of the site recognised the local authority-approved equipment. When questioned, the supervisor claimed the items were previously used and had been taken from homes while they were being replaced by new equipment. However, a number of the items were sold with information suggesting they were guaranteed for at least a decade from point of sale.

COVID Lessons: The pandemic has created an exponential growth in online sales. Furthermore, the budgets for purchases of attractive items were probably set before the business interruption kicked in and consequently there can be unplanned/unidentified stocks of such assets which it has not been possible to use. These factors negate the effectiveness of two of the key counter fraud controls: budget monitoring and changes in usage profiles.

Cyber Fraud

Cyber Crime continues to rise in scale and complexity at an alarming pace, and affects businesses and individuals alike, costing the UK billions of pounds. The aim of the cyber criminals is to obtain personal and sensitive data for financial gain.

Cyber crime falls into two distinct categories:



Cyber-Enabled Crimes

These are traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT. An example is data theft.

Cyber-Dependent Crimes

These are crimes that are committed only through the use of ICT devices, where the devices are both the tool for committing the crime, and the target of the crime. An example is developing malware for financial gain.

Cyber Risks

There are a number of recent publicised cases of cyber attacks on councils. Many of these would appear to be service-denial and/or data harvesting cases, rather than for direct fraudulent benefit.

The emergence of remote working and the consequential increase in the use of digital authorisation, provides a fertile opportunity for cyber-fraudsters to exploit. We have seen examples of this where approvals and similar are being made on the strength of an email, with very limited corroboratory work done to confirm the authenticity of the email itself.

The use of propriety software to evidence the signature of an authorising officer is one means by which the risks associated with email interception/cloning can be mitigated. This type of software can also be extended to verify external authorisations for significant electronic transactions such as refunds, requests for interim payments, etc. This type of software provides multiple methods to authenticate the signer including Access Code (similar to a password), SMS code, phone call, or Knowledge-Based Authentication.

Attractive items which are currently particularly vulnerable

Many frauds require there to be a market for the items which are being stolen. The COVID pandemic has seen temporary shortages of a number of items. This in turn has increased their value in the online market place and also reduced the diligence checks prospective purchasers might otherwise perform.

Examples of both new and also used items include:

- Laptops
- Flat screen monitors
- Building materials
- Office furniture

If you require any proactive or reactive counter fraud support or assistance, then please contact

Melanie Alflatt, Director of Anti-Crime Services

Email: **fraud@tiaa.co.uk**

www.tiaa.co.uk

0845 300 3333