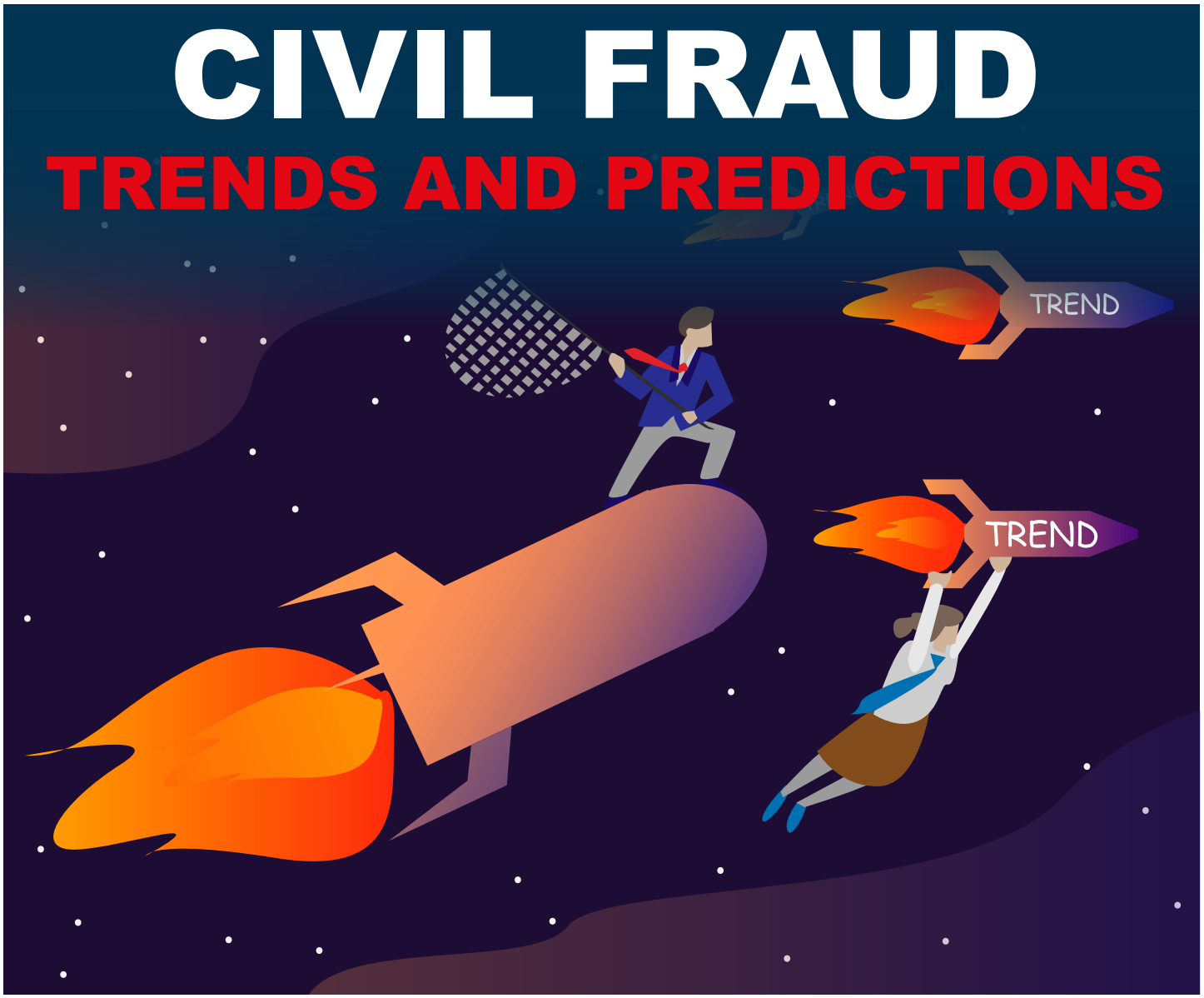
CIVIL FRAUD

TRENDS AND PREDICTIONS



Authored by: Emma Allen and Lorna Bramich - Taylor Wessing

In times of economic uncertainty, fraud typically increases. And these are certainly economically uncertain times. Fraud has been on the rise over recent years and that trend is set to continue. The motivation and opportunity to commit fraud increases as financial pressures loom over individuals and businesses. We are also set to see a continued increase in insolvencies as the impact of the pandemic and other global events set in. The appointment of insolvency practitioners means frauds which might have otherwise continued or remained concealed are more likely to be uncovered. With all of this in mind, a crystal ball is not required to predict that we are likely to see a significant uptick in fraud-based claims emerging over the next 12-24 months. In this article we consider some of the key trends and predictions for civil fraud.

1. Authorised push payment (APP) fraud

APP fraud has been a consistent feature of the civil fraud landscape for the past few years, and it isn't going away.

The Payment Systems Regulator recently reported that instances of APP fraud increased 39% between 2020 and 2021, making it the largest type of payment fraud and most prevalent crime in the UK.

Where businesses are targeted, APP frauds often involve a fraudster hacking into and monitoring an email account or server to identify regular payments (such as to a supplier or contractual counterparty) and accounts departments responsible for the receipt and processing of invoices. This is to identify transactions they can manipulate by replicating an invoice,

replacing payee account details with their own fraudulent details, and sending the fake invoice from a genuine (hacked) email account or a fake domain name which resembles the genuine account such that recipients glancing at the sender address may not pick it up. These invoices are then paid with the organisation unknowingly sending its funds to fraudsters.

In our experience, fraudsters will go to great lengths to ensure the invoice gets paid, including forging KYC documentation to enable them to clear the innocent party's internal payment processes regarding account detail changes. Often, by the time the innocent party realises they have paid the wrong person (which sometimes isn't until the supplier starts chasing for payment of an outstanding invoice), several days or more have passed and the prospects of recovering the full amount are slim, although they improve if decisive action is taken as soon as the fraud is discovered.

Where individuals are concerned, tactics employed by fraudsters can include phishing emails and texts, creating fake or cloned websites or social media accounts purporting to provide investment opportunities or to sell products to consumers, or more elaborate ploys like in the well-known case of Phillip v Barclays where a group of fraudsters convinced Dr and Mrs Phillip that they worked for the Financial Conduct Authority and were acting in conjunction with the National Crime Agency to protect the Phillips's life savings by moving them to a safe account.

Victims of APP fraud are increasingly looking in the direction of banks for reimbursement – usually their own bank but also sometimes the receiving bank. The Quincecare duty has been something of a trending cause of action over the past few years, and will no doubt continue to be considered by claimants – after all, a bank is a much more attractive potential defendant than a fraudster. Cases such as Tecnimont Arabia Limited v National Westminster Bank PLC [2022] EWHC 1172 (Comm)) also demonstrate that claimants are prepared to make claims against the receiving bank (ie the alleged fraudster's bank) to recover their funds, albeit that such an approach remains challenging.

The Payment Systems Regulator is strongly encouraging banks to increase monitoring of inbound and outbound payments to address the need to reduce the impact of APP fraud. It is currently undertaking a consultation on APP fraud reimbursement and has proposed that there should be mandatory reimbursement unless it can be shown that the victim has been grossly negligent. The proposed starting point is that the reimbursement liability should be shared on a 50:50 basis between the sending and receiving banks. Watch this space.

2. Crypto fraud

Whilst the vast majority of crypto asset use is for legitimate purposes, crypto-related fraud continues to hit the headlines.

October 2022 was dubbed 'hacktober' in the crypto press following a Chainalysis report that US$718m had been stolen from DeFi protocols in 11 hacks by the middle of the month.

The majority related the US$570 Binance Bridge hack. Mango Markets, a defi platform, also suffered major losses when it was targeted by an attacker who exploited an 'economic design flaw' in the protocol to manipulate the price of the native token and then borrow against that inflated value from the Mango treasury, draining around $117m from the US$190m of deposits available on the platform.

DeFi bridges and protocol vulnerabilities will continue to present opportunities for fraud, and expect to continue to see rug pulls, pump and dump scams and wallet data breaches.

Crypto exchanges should prepare for an increase in claims being made directly against them where the proceeds of crypto fraud can be traced into that exchange. In D'Aloia v Persons Unknown and Others [2022] EWHC 1723 (Ch), the court held that the claimant, whose crypto assets had been fraudulently misappropriated, had a good arguable case in respect of a constructive trust claim as against the exchanges which were understood to be holding the proceeds of the fraud. The judge noted that once the relevant defendant exchanges (or their holding companies) were notified of the judgment, they were likely to "come under the duties of a constructive trustee for the claimant in respect of those crypto assets", potentially opening the door to a direct claim against the exchange and its controlling entities if it breaches its duties.

3. Investment fraud

During the COVID-19 pandemic, the SEC issued an investor alert warning that it had experienced a significant uptick in complaints and tips relating to investment fraud, such as Ponzi schemes. Action Fraud in the UK issued a similar warning.

Investment frauds are one of the oldest scams in the book and include companies persuading individuals to transfer their pension pots to their - often high-risk - investment products on the promise of high returns, only to see their life savings disappear. Often these frauds aren't uncovered until the scheme collapses into an insolvency process. Given the current macro-economic environment, we expect to see an increase in high profile litigation arising out of investment fraud, and those claims are likely to sit in the hands of an insolvency practitioner.

4. Supply chain fraud

Supply chain pressures have also been exacerbated by the pandemic and general economic outlook. The phrase 'supply chain fraud' covers a plethora of potential claims including bribery and corruption, inventory and warehouse fraud (where receipts for the same goods/commodities are used more than once to raise finance), asset misappropriation and falsifying sales.

In a global market, supply chains are increasingly international and that makes them much more difficult to oversee. There may be multiple third party subcontractors, suppliers and vendors involved in an international supply chain which increases the risk profile for fraud.

5. False accounting

Some of the largest frauds in recent years have been accounting frauds involving the inflation of assets and revenue and keeping debt off balance sheet – aka 'cooking the books'. Supply chain fraud and fraudulent accounting are often seen together, for example where procurement employees enter into arrangements with suppliers which are either improperly accounted for, circumvent internal systems and controls or result in some personal gain such as a kickback. With financial pressures increasing across the board, this type of fraud is set to continue and increase.

In the longer term, we also expect to see an increase in ESG related false reporting, specifically in relation to climate related financial disclosures. There is an ongoing formalisation of reporting requirements, with mandatory disclosure requirements now in place for certain types of business following the Companies (Strategic Report) (Climate-related Financial Disclosure) Regulations 2022 and amendments to certain sections of the Companies Act 2006 (sections 414C, 414CA and 414CB).

6. Insolvency claims

As company insolvencies rise, it is inevitable that there will be an increase in instances of fraud being unearthed which would otherwise have remained concealed. For example, fraud relating to the COVID-19 government support schemes is likely to become more apparent as insolvencies increase. At the end of last year, the Department of Business, Energy & Industrial Strategy estimated that £4.9 billion issued through the Bounce Back Loan Scheme alone was lost to fraud.

Fraud claims can be difficult to prove and costly to pursue, but the appointment of an insolvency practitioner is often advantageous where fraud has occurred because an additional set of tools becomes available for investigating and bringing claims. For example, insolvency practitioners have broad investigative powers (such as under s236 of the Insolvency Act 1986), and may be able to challenge transactions at an undervalue or as preferences, or where assets have been moved out of the reach of creditors, insolvency practitioners (or victims) may be able to bring a claim pursuant to section 423 of the Insolvency Act (transactions defrauding creditors) to recover their losses, which does not require any proof of any form of dishonesty and can therefore compare favourably to a fraud-based claim in terms of the evidential burden on the claimant.

The Economic Crime and Corporate Transparency Bill, which had its first parliamentary reading in September 2022, is another development to watch in both a fraud and insolvency context. The Association of Business Recovery Professionals, R3, recently commented on the Bill and recommended that the company dissolution process be changed so that before a company can be dissolved it must be placed into an insolvency process to allow appropriate investigations into the company's affairs to be undertaken. If these changes are implemented, this will increase the number of insolvencies which could in turn lead to an increase in the number of fraud-based claims brought by insolvency practitioners.