cifas
Fighting Economic Crime Together

FRAUDSCAPE 2023

Welcome to Fraudscape 2023

Welcome to this year's edition of Fraudscape, which sets out the challenges and threats facing the fraud prevention community, and the areas on which we need to focus to fight fraud and financial crime together more effectively.

This report combines data from our National Fraud Database (NFD) and Internal Fraud Database (IFD), along with intelligence provided by Cifas members, partners and law enforcement. In 2022, our members prevented more than £1.3bn of fraud losses through the use of the NFD but we know we can help prevent and detect even more fraud and financial crime by developing a better understanding of key threats and enablers – which is the main purpose of this report.

Continuing uncertainty around the UK economy, the rise in the cost of living, and the increasing number of employees now working from home have provided a rich seam of opportunity for exploitation by criminals. These circumstances have also increased incentives for those who may be struggling financially to commit fraud in order to generate additional income during these difficult times. The trends that we have identified in 2022 are continuing into 2023 and we continue to see an increased risk of identity theft, first party fraud and internal fraud.

This background means that our role in protecting our members, the public, and the wider UK economy from fraud and financial crime is

more important than ever. As the threat continues to evolve and threat actors innovate in order to fraudulently open and abuse accounts, steal identities and take over customer accounts, Cifas will accelerate development of new products and services to protect businesses and consumers.
We will also continue to educate young people and give them the skills to recognise the serious consequences of financial crime through our counter fraud lesson plans, and roll out our counter fraud training to many more employees, recognising their important role as the first line of defence against fraud and financial crime.

The sharing of data and intelligence across a broader coalition of organisations is one of the most effective defences we can put in place to prevent fraud, and Cifas is proud to bring together the counter fraud community from multiple sectors to create that defensive wall. Only by working together can we stem the rising tide of fraud and financial crime.

I hope that you find our analysis insightful and, more importantly, a call to action to strengthen your defences against fraud and financial crime.

Mike Haley, CEO, Cifas

Overview

- 2022 saw an unprecedented 409,000 cases of fraudulent conduct recorded to the NFD – the highest volume of cases ever recorded. This is an increase of 14% (+48,840) on 2021 and up 12% (+44,738) on the number of cases recorded pre-pandemic.

- The highest ever volume of identity fraud cases was recorded in 2022 – over 277,000 cases. This is up by nearly a quarter – 23% – on 2021 and accounts for 68% of all cases on the NFD.

- Misuse of facility is the second highest recorded case type, with over 70,000 cases – down 11% on 2021. Although a large proportion of cases are related to bank accounts, there has been an increase within the loans and plastic card sector.

- 68% of misuse of facility cases on bank accounts have intelligence indicative of money mule activity. The key age range for this continues to be 21-25 years, with social media a key enabler in the recruitment of mules.

- False application increased by 40% compared to 2021, with nearly 24,000 cases, which is back to pre-pandemic levels. False documents are an issue, with a rise in false utility bills provided in false applications for products and services.

- Levels of facility takeover are similar to 2021, with over 37,000 cases recorded. The online retail and telecom sectors are primarily targeted for facility takeover, as threat actors look to take over existing accounts to order goods to sell on.

- 294 individuals were recorded to the IFD, an increase of 9% on 2021, with employment application (unsuccessful) the main case type. A large number of these cases are related to concealment of information, such as hiding adverse credit history or employment history. The combination of rising living costs and remote working is a key challenge as employees may be tempted to supplement their incomes from dishonest conduct.

Identity Fraud

- Identity fraud rose by nearly a quarter – 23% – in 2022 compared to 2021 (+51,499). Identity fraud cases have now reached an unprecedented level, accounting for 68% (277,234) of cases in 2022.

- Impersonation – current address fraud accounts for 74% of filing reasons (206,534) and is up 16% on 2021 (+27,855). This filing reason is linked heavily to the plastic card sector, which has seen a 37% increase in 2022 (+13,390). There has been an 84% rise (+5,887) in false identities with organisations reporting the increased use of synthetic identities.

- 86% of identity fraud occurs through online channels, though there was a significant increase in cases linked to retailers (+132%, +9,732) and dealers (+246%, +4,530). This may be a direct result of threat actors trying to circumvent online identity verification controls.

- Threat actors continue to target plastic cards in order to purchase goods that can be sold on. There has also been a rise in identity fraud against telecom products, where victim identities are used to purchase mobile phones to sell on.

- Most victims are over 31 years, with those aged 61+ also seeing significant increases.

Organisations face numerous challenges as they try to stem the tide of identity fraud.

The increasing use of synthetic identities and deep fakes to try and access products and services is a considerable threat. Reports from Cifas Intelligence suggest that threat actors are going to considerable effort to use synthetic identities over long periods to build credit reports in order to pass know your customer checks. This type of activity is supported by false documents such as driving licences and utility bills, and document manipulation using photo editing software.

Smishing campaigns featuring text messages claiming to be the fraud team at a bank, or utilising messaging services such as WhatsApp posing as a friend or family member, remain a key enabler for threat actors to gather personal information and/or access to accounts. During 2022, organisations reported that their staff were impersonated on sites such as LinkedIn in order to target customers to harvest personal details.

Though a standard method of attack, phishing emails containing links to malicious sites to harvest personal and financial information continue to provide a rich seam of information for threat actors. Throughout 2022, phishing emails were used to target consumers, with the energy crisis providing an opportunity to imitate utility companies and offer deals, grants or loans to help with the cost of living. According to the Telephone Operated Crime Survey for England and Wales (TCSEW)[1], those between 25-44 years were more likely to be targeted, with half of all adults reportedly receiving a phishing email in the month prior to the survey. According to the TCSEW, of those who replied or clicked on a link in a phishing message, more than a third (35%) said they did so for financial or material gain, and 30% to pay an invoice or bill.

Cybercrime as a service platforms are growing and utilising deepfake technology to dupe social media users. One example is software for hire that can control over 30,000 fake online profiles[2] that can be used to create accounts on sites such as Twitter, LinkedIn, Facebook, Telegram, Gmail, Instagram and YouTube. Some even have associated Amazon accounts with credit cards, bitcoin wallets and Airbnb accounts. This can easily be used to socially engineer individuals into revealing their personal and financial information.

Deepfake technology is a growing concern, with deepfake videos increasing at an annual rate of 900%[3]. This technology can be used in videos, photos for selfies and for voice recognition. Organisations have started to see the manipulation of selfies for onboarding purposes, utilising face swapping technology to replace the real face in the original image with the selected one from another. Deepfake technology can also be supplemented by artificial intelligence such as ChatGPT[4] which can write scripts to respond to certain scenarios.

---

[1] Phishing attacks – who is most at risk? - Office for National Statistics (ons.gov.uk)
[2] 'Aims': the software for hire that can control 30,000 fake online profiles | Technology | The Guardian
[3] Deepfakes: What they are and tips to spot them | Tripwire
[4] ChatGPT broke the EU plan to regulate AI – POLITICO

Misuse of facility

- Misuse of facility is the second highest recorded case type, with over 70,000 cases – down 11% (-9,071) on 2021. Although a large proportion of cases relate to bank accounts, there was an increase within the loans and plastic card sector. In addition, there has been a growth in evasion of payment as well as fraudulent chargeback claims – which may be reflective of the current economic climate.

- Misuse of loan products saw a 114% increase (+1,387) and plastic cards a 28% increase (+1,091) in 2022.

- In 2022, 39,578 cases on bank accounts were recorded that hold intelligence indicative of money mule behaviour. This is a reduction from 2021 (-21%). However, these cases still account for 68% of misuse of bank accounts.

- Although personal current accounts are mainly targeted (87% of products), there has been a 35% increase in personal savings – instant/easy access (+221).

- The key age range for mule activity continues to be 21-25 years, with social media remaining a key enabler in the recruitment of mules.

There are a number of key enablers identified in 2022 that are driving misuse of facility. Fraud bibles, which are available on social media and other forums, provide guidance to individuals on how to commit different types of fraud. Various social media and online gaming platforms continue to be used to recruit individuals to become money mules. Organised crime groups recruiting students also continue to be an enabler and challenge for the fraud prevention community to mitigate.

As living standards continue to decline, there is a risk that the perception of fraud among the public may change. For example, individuals may be tempted to falsely claim items were not delivered, dispute transactions or try to exploit refund policies by falsely claiming goods and services were non-satisfactory. Cifas research in 2022[1] revealed that one in five people (20%) admitted that they or someone they knew had committed non-delivery fraud over the last 12 months – up from 18% in 2021. Similarly, money mule recruitment tactics sought to exploit the cost of living crisis by framing advertisements offering help to those struggling with bills. This trend may be exacerbated by individuals becoming more receptive to this type of advertisement as they look to supplement incomes.

Disputing transactions and refund as a service are two threats that have developed over 2022 and remain a key risk into 2023. There are numerous instances of customers disputing transactions and historic investment transactions claiming they had not authorised them. This is supplemented by third-party claims management companies contacting banks on behalf of customers to dispute charges whilst attempting to limit contact between the bank and the customer. In many instances, customers appear

to have been coached by the claims management companies on what to say to support the dispute. There has also been an increase in adverts offering help to consumers to falsely claim a refund. These usually charge between 10%-30% of the total refund value[2]. The services vary from did not arrive – falsely claiming the goods were not delivered – to boxing services that perform label manipulation and postage for refund fraud services.

Fraud forums and dark web marketplaces remain a concern for the fraud prevention community. Adverts offering to rent UK personal bank accounts for monthly payments of cryptocurrency equivalent to 200 dollars per month have been seen across several forums. Threat actors express an exclusive interest in mainstream UK bank accounts and provide a structured process for anyone who agrees to allow access to their account. Additional payments are being offered where there is a requirement for the genuine account holder to communicate with their bank, suggesting an awareness of biometric controls and other detection controls. There is also coaching provided for individuals if they are contacted by the bank.

Cashing out using crypto wallets and other digital wallets continues to be a preferred method of mule herders, who actively seek out those with crypto wallets and abuse digital platforms such as Skrill to cash out.

---

[1] Cifas research reveals increase in shoppers committing non-delivery fraud I cifas
[2] Refund fraud-as-a-service ads on hacker forums increase by 60% (darkreading.com)

Facility takeover

- Cases of facility takeover in 2022 are similar to volumes in 2021 (37,285 vs 37,305 cases).

- Online retail is the most targeted product (38% of cases in 2022). This is due to many retailers offering credit before payment. Demand for credit card usage grew in 2022, highlighting increasing household reliance on credit as rising prices squeezed finances.

- The telecom sector is the second most targeted sector (29% of cases). Of note is the 37% increase in plastic cards and, in particular, personal credit cards. A large number of these cases relate to unauthorised security/personal details change (49%).

- Overall, unauthorised security/personal details change accounts for 57% of filing reasons and is up 72% on last year (+8,859). This filing reason has mainly been used by the online retail sector.

- Social engineering is a key enabler of facility takeover as threat actors engineer consumer and contact centre staff to understand the verification process in order to take over accounts. 64% of facility takeover cases occur through online channels and 26% through telephony channels.

- Overall, most victims are over 41 years.

While levels of facility takeover have remained consistent with 2021, threat actors are exploiting an evolving range of threats to take over accounts.

Data breaches remain a key route for the harvesting of personal information, exacerbated by some consumers using the same login details for multiple services. This has resulted in several account takeovers where the genuine customer details had previously been involved in another data breach.

Malicious codes deployed into apps such as QR code scanners infect devices and harvest credentials used to log in to certain platforms as well as intercept any multi-factor authentication that service providers use to protect customers. Threat actors have also set up number of websites spoofing popular brands to harvest personal and financial information from genuine customers. These website URLs are similar in name, utilising a different character – such as 'ɑ' instead of 'a'.

Customers are then directed to a malicious website and often instructed to download a fake app which will infect their device with malware.

Threat actors are cold calling consumers offering an opportunity to upgrade a handset or to offer discounts on a new contract. Customers are socially engineered to reveal personal details and orders are placed for a different handset to that initially offered. Following delivery, the victim is advised to return the wrong device to an alternative address, with communication often made through WhatsApp.

There have been increasing reports of threat actors calling contact centre agents on multiple occasions to understand the verification process. They have then used the information learned about the process to target consumers, even mimicking the hold music used by the contact centre. These details are then used to social engineer the contact centre staff to gain access to the account. Research suggests that 60% of fraud involves a contact centre, even if the fraud attempt occurred through another channel, with an average of 26 phone calls made leading up to an attack . Threat actors may also target interactive voice response (automated phone system technology that allows incoming callers to access information via a voice response system of pre-recorded messages) used by contact centres to extract information.

As a result of tighter controls being placed on affordability for credit facilities such as buy now pay later, threat actors are likely to try and utilise existing accounts. HM Treasury's requirement that lenders should carry out more affordability checks may prompt threat actors to turn their attention towards existing products and services, utilising personal information stolen from data breaches to socially engineer customers and target accounts that have good available credit.

---

[1] Fraudsters ♡ contact centres. Here's how to keep them at bay... (finextra.com)
[2] Buy-now pay-later firms face clampdown under new rules - BBC News

Insider threat

- 294 individuals were recorded to the IFD in 2022 – an increase of 9% from 2021 (268).
- 42% of cases are false employment application (unsuccessful), which is up 22% (+26) from 2021. Cases are mainly in relation to concealment of information, such as hidden adverse credit history (49%), address with adverse (14%) or employment history (12%).
- 39% of cases are dishonest actions, which is up slightly by 2% (+2) from 2021. Cases of dishonest actions are mainly linked to theft related incidents, such as theft of cash from employer (13%), theft of IT equipment (8%) and theft of cash from customer (7%).
- 57% of cases are discovered through internal controls (167), but there was a 27% increase in reports being made by the customer (+6).
- Most individuals are between 21-30 years (44%), although there has been a 16% rise in those between 31-40 years (+15).
- False references have significantly increased in 2022 (+375%, +15), which is largely in relation to the use of reference houses to facilitate false applications for employment in financial institutions.

Over the past few years the job market and ways of working have changed considerably, creating new types of risk for organisations to deal with. External factors such as the cost of living crisis and high interest rates have also added additional challenges.

Fake employment agencies were created and used to facilitate fraudulent job applications, including false references and employment history, and to fabricate experience. Agencies often attempt to place candidates in roles with access to sensitive customer data e.g. know your customer positions. 2022 has seen an increase in reporting of reference houses that provide false references and documents for job applicants. With the rise in living costs and job seekers desperate for well paid roles, individuals may be more inclined to use these services when applying for jobs.

Remote working (including abroad) is one of the key risks facing organisations. Long periods of isolation without regular contact and support are known to be associated with security mistakes and increased vulnerability to social engineering tactics. Remote working has also led to challenges around monitoring staff, which have been exploited by employees who have remotely accessed customer data and then sold it on. As the cost of living crisis continues, organisations are reporting an increasing number of instances of staff abusing processes to redirect payments, apply credits and dispute personal spend. Staff have also abused employee referral schemes to obtain cash bonuses.
Employees who are financially struggling could rationalise decisions to engage in dishonest conduct. This is supported by organisations reporting staff committing dishonest conduct to supplement their income or to obtain employment.

Several organisations have reported inconsistencies with employment applications, particularly in relation to concealment of information and adverse credit history. Candidates are concealing information about their financial and employment history to make them more attractive to potential employers and, in some circumstances, have created fake LinkedIn profiles to make themselves seem more suitable for the roles for which they are applying. Cifas research shows that 10% of UK adults have lied about their degree qualification in the last twelve months, compared with 8% in 2021 .

[1] Nearly a tenth of Brits admit they've lied on their CV in the last 12 months | Cifas

False application

- 23,819 cases of false application were recorded in 2022, a rise of 40% compared with 2021. Increases were seen within the bank account sector, mortgage sector, asset finance and loans.
- False documents account for 39% of filing reasons for false application and have risen by 109% (+4,840).
- 77% of false applications came through online channels, but there has been an increase in applications coming through combined channels – such as online applications being finalised in branch (+188%, +261). There has also been a rise in face-to-face channels (+27%, +198).
- A large proportion of false documents identified in false applications are utility bills (40%) followed by bank statements (22%). The rise in false utility bills mainly relates to bank accounts.

2022 has seen sustained growth in consumer credit usage with levels the same – if not higher – than before the pandemic. As more people look to apply for products and services for financial support during the rising cost of living, they may also be tempted to falsify information to make themselves appear more credit-worthy or hide previous adverse information.

False applications have been enabled a number of ways including:

PDF manipulation software: available online, easily enables document manipulation

Unregulated brokers: third parties making applications through direct channels with false documentation

Abuse of Companies House: false companies being registered to support false applications

The rise in living costs has changed consumer behaviour. Research suggests that for products such as insurance, 33% of motorists have changed at least one material detail on their insurance application to save money and 17% admit to insuring a car in their name, even if someone else (such as their child) is the main driver. Application fronting is still a key issue for several sectors, particularly asset finance, loans and insurance.

Some of the challenges are not just around evidencing application fronting, but challenges from the Financial Ombudsman Service, particularly regarding family fronting. It is difficult to prove, but also has a number of challenges when a dealer is involved.
Sectors that offer credit facilities are seeing an increase in applications

showing falsified income, as well as applicants allegedly being employed by a family business when they are not. We suspect applicants are falsifying information to influence lenders' decision making in the challenging economic climate.

The abuse of Companies House remains a key threat, as false companies are incepted to help support applications for grants and loans. Whilst the Economic Crime and Corporate Transparency Bill will set out reforms to Companies House verification checks, in the interim it remains a highly targeted public register. Threat actors will also create fake websites and LinkedIn profiles to add legitimacy to the business presence.

---

[1] Equifax Pulse Market Webinar, 7th December 2022
[2] https://www.aviva.com/newsroom/news-releases/2022/12/aviva-reports-16-percent-rise-in-application-fraud-over-same-period-in-2021/
[3] Economic Crime and Corporate Transparency Bill - Parliamentary Bills - UK Parliament

Summary

- Over 409,000 cases to the NFD in 2022 – the highest level ever recorded.

- 68% of cases concerned identity fraud, demonstrating the challenge organisations face in verifying customers through digital channels. There was also rise in the use of synthetic identities to access products and deep fake technology used in document manipulation and voice manipulation. In 2023 it is important that organisations use a layered approach to verification to make it as difficult as possible for synthetic identities to be used.

- High inflation in the UK may lead to more consumers becoming susceptible to phishing and smishing campaigns offering services to help with finances. There is an increased risk that threat actors will target consumers with existing products as lenders tighten affordability criteria on new applications due to economic uncertainty and high interest rates.

- Social engineering of customers remains a common tactic, but there is increasing evidence of technology-driven threats, such as bot attacks targeting organisations to access customer accounts.

- First party fraud will be an increasing threat in 2023 as consumers attempt to appear more creditworthy or are tempted to commit fraud to cope with rising living costs.

- Challenging perceptions of first party fraud among consumers will require a cross-industry approach. The number of consumers falsely claiming a chargeback increased significantly over the last year, and there are guides available online providing instructions on how to commit such fraudulent conduct.

- There is scope for an increase in authorised push payment fraud as consumers are targeted with false investment opportunities to generate income.

- Mule recruitment will continue to be a challenge as mule recruiters convince account holders there will be no consequences for taking part in this type of activity, and coach them on how to respond if challenged by a bank.

- The insider threat should also be a priority due to the financial struggles brought about by the cost of living crisis that many employees may be experiencing.

- Remote working has also made it difficult to manage the insider threat risk. It is essential that organisations carry out regular screening of staff and contractors, as well as wellbeing checks, to help mitigate these risks.

What do the findings tell us?

Cifas members recorded over 409,000 cases to the NFD in 2022. 68% of these cases concerned identity fraud, which demonstrated the challenge members face verifying customers particularly through digital channels. We also saw a rise in the use of synthetic identities to access products and deep fake technology used in document manipulation and voice manipulation. As inflation in the UK hits a 10 year high, consumers may be more susceptible to phishing and smishing campaigns by threat actors offering services to help with their finances. There is also a risk that consumers with existing products will be increasingly targeted by threat actors as affordability checks on new applications make it more difficult to access new products due to economic uncertainty and high interest rates. Social engineering of customers remains a common tactic, but there is increasing evidence of technology-driven threats such as bot attacks targeting organisations to gain access to customer accounts.

First party fraud is likely to be an increasing threat members will face in 2023 as individuals attempt to make themselves more credit-worthy or look to cope with rising living costs. There is potential for an increase in authorised push payment fraud as consumers are targeted with false investment opportunities to generate income. Mule recruitment will continue to be a challenge for members, as mule recruiters convince account holders there will be no consequences for taking part in this type of activity, and coach them on how to respond if challenged by a bank.

Challenging perceptions of first party fraud will require a cross-industry approach. The number of individuals falsely claiming a chargeback has increased significantly over the last year, and there are a number of guides available online providing instructions on how to commit such fraud.
As a result, it is essential that organisations consider diversifying their customer authentication checks to counter this type of threat.

The insider threat should also be a priority for members due to the financial struggles that many employees may be experiencing due to the cost of living crisis. Remote working has also made it difficult to manage the insider threat risk, so it is essential that members carry out regular screening of staff and contractors, as well as wellbeing checks to help mitigate these risks.

Recommendations

1. **It is important that we fully understand the scale of the problem we face. Only through reporting can we fully understand the nature and size of the threat the UK faces and adjust our response accordingly. Find out how to report below.**
    - **Report scam emails here**
    - **Report scam texts here**
    - **Report a scam website here**
    - **Report fraud here**
    - **Report tax scams here**

2. Rising living costs, high inflation and interest rates may push consumers to commit fraudulent conduct. It is important that we coordinate our messaging to deter people and ensure they understand the consequences of engaging in fraudulent activity.

3. Members of the public are at more risk than ever of falling victim to fraud and scams. It is important that we encourage the public to take proactive steps to protect themselves, as outlined in the Take 5 campaign.

4. Businesses should ensure that they have robust cyber risk management protocols in place to protect themselves and their customers. There is a variety of information and tools that can support businesses and a selection are listed below.
    a. Global Cyber Alliance
    b. National Cyber Security Centre
    c. Police Cyber Alarm

Extra Content

We are Cifas – we protect organisations from fraud and financial crime. We provide a range of financial crime prevention solutions. For over 30 years we have been trusted by our partners to provide them with the systems and tools they need to detect and prevent fraud and financial crime, saving them billions of pounds in prevented losses.

We are a not-for-profit membership organisation that brings different sectors together for the common goal of eliminating fraud and financial crime. Over 600 organisations work with us, all benefiting from each other's data, intelligence and learning – using the cutting edge financial crime prevention systems and tools we develop and deliver.

Press

For any press enquiries please contact press@cifas.org.uk

About Cifas

- If you are interested in joining Cifas click here.
- For more information about our digital learning, courses and qualifications click here.
- Want to know when new content is added – register to be notified here.