cifas
Fighting Economic Crime Together

Fraudscape 2024

Fighting Fraud and Financial Crime Together

Pioneering intelligence, analysis and statistics to illuminate the fraud and financial crime landscape, and direct our shared strategic response to the threats.

Welcome

Welcome to this year's edition of Fraudscape, which sets out the challenges and threats facing the fraud prevention community, as well as 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 Insider Threat Database (ITD), along with intelligence provided by Cifas members, partners and law enforcement.

In 2023, our members prevented more than £1.8 billion of fraud losses, 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. The information and intelligence included in Fraudscape is key to us doing that.

Continuing uncertainty around the UK economy, the rise in the cost of living, and the growth in hybrid working has provided a rich seam of opportunity for criminals to exploit. These circumstances have also increased incentives for those who may be struggling financially to commit fraud to generate additional income. The fraud trends we identified in 2023 continue into 2024, with an increased risk of identity theft, first party fraud and internal fraud.

Against this background, our role in protecting members, the public, and the wider UK economy from fraud and financial crime is now more important than ever. As the threat continues to evolve and threat actors innovate 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 to provide them with 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 we are proud to bring together a community of organisations from a wide variety of sectors to create a defensive wall against fraud.

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

374,160 cases recorded to the NFD in 2023

Identity fraud cases account for 64% of all filings

Overview

Following a surge of cases in 2022 (over 400,000 – the highest ever recorded), filings to the National Fraud Database (NFD) fell by 9% in 2023 to 374,160 cases. Despite this reduction, there were increases across the categories of facility takeover (+13%) and misuse of facility (+5%). Key increases in 2023 include a rise in asset conversion cases (+55%) and cases of facility takeover (+13%), particularly against telecommunication products and personal credit cards.

Misuse of facility now accounts for one in five cases on the NFD (previously 17%) with the increase centred on pre-paid cards, asset finance-hire purchase, and Coronavirus Business Interruption Loans (CBILs) filings.

Moreover, NFD filings remain higher than 2021 by 4% (nearly 14,000 cases), with organisations recording a case to the NFD every two minutes, on average. Market conditions and the tightening of controls and lending criteria due to economic uncertainty, may be a driver behind the decline in filings in 2023.

Identity fraud continues to be the dominant case type recorded to the NFD (64% of filings, 237,642 cases). Increases were observed across personal bank accounts (+12%) with concerns centred on social media enablers and the growing threat of AI and sophisticated data harvesting techniques designed to exploit an array of cost-of-living pressures.

One in ten cases relate to facility takeover, which saw the largest volume increase across all case types (+4,809, +13%). Intelligence and NFD data support a shift in tactics, with threat actors increasingly targeting existing accounts to obtain new products or upgrades, particularly within the telecommunications sector.

Misuse of facility remains the second most dominant case type, now accounting for 21% of filings (73,459 cases), following a rise of 5%. A key driver is evasion of payment across several products. There was a 6% reduction in cases that held intelligence indicative of money muling, however, these cases still account for 65% of misuse of bank account filings.

False application cases fell by 17% overall, but there was an uplift against the loan (+36%), insurance (+20%) and telecommunication sectors (+17%). False documents (usually bank statements and utility bills) are the dominant filing reasons, with individuals filed for providing false information or omitting details to obtain products and services.

Filings to the Insider Threat Database (ITD) increased by 14% in 2023. The rise is focused on dishonest action by employees (49%), with many organisations citing increasing financial pressures as a driving factor behind the uplift. Most individuals filed to the ITD (38%) had been in their position for less than a year (previously 21%). This could be an early indication that employees are more willing to risk engaging in dishonest conduct in the early stages of employment although, equally, there are signs of improved controls and staff awareness, with cases detected by internal controls and staff up by 20% and 44% respectively.

Case of facility takeover increased by 13% in 2023

Insider threat filings increased by 14% in 2023

Identity fraud

Identity fraud cases are down 14% following a reduction across several sectors. However, identity fraud remains the dominant case type, accounting for 64% of filings (237,642 cases) in 2023; a slight decrease as a proportion of total filings compared to 2022 (68%).

Despite the overall reduction, bank accounts observed the largest increase (up 12%, +5,811), with personal current accounts being the most targeted. Plastic cards continue to be the most afflicted product, but also observed an 8% decrease.

The most notable reduction by volume was across telecommunications products (-49%) which can, in part, be explained by a shift in criminals targeting these products via facility takeover activity, as opposed to identity fraud.

Overall, impersonation involving a current address fraud accounts for 77% of filing reasons, however, this has decreased 11% compared to 2022.

Most victims of impersonation filed to the NFD continue to be over 61 years (accounting for 24%) in both 2022 and 2023, followed by 51-60 years (21%).

Of note, those aged 21-30 years saw an 11% increase. This is mainly linked to impersonations for mobile phones, personal credit cards and current accounts.

Identity fraud involving bank accounts increased by 12%

Most victims of impersonation are over 61yrs

Impersonation current address fraud accounts for 77% of filing reasons

Misuse of facility

In 2023, organisations filed 73,459 cases of misuse of facility. This represents a 5% increase (+3,261) compared to 2022.

Whilst bank accounts recorded a decrease (-2%), loan products recorded a notable increase (+82%), followed by asset finance (+45%) and plastic cards (+17%). Increases across loan products were due to an uplift in evasion payment of loans issued under the CBILs scheme (+2,727), whilst asset finance cases were centred on theft of assets and evasion of payment.

These increases were spread across several organisations, highlighting the impact of the cost-of-living pressures and individuals looking to avoid payments or financially gain from stealing assets.

Deep Dive - Money Mules

In 2023, 37,261 cases were recorded to the NFD that held intelligence indicative of money mule behaviour. This is down 6% from 2022 (39,611 cases).

Despite the reduction, these cases still account for 65% of misuse of bank account filings recorded to the NFD. Personal current accounts continue to be the dominant product impacted, accounting for 90% (previously 87%).

Company current accounts observed a small reduction (-9%) and continue to account for just 6% of filings overall.

Where recorded, most individuals filed for this type of behaviour are aged between 21-25 years (23%), which is consistent with 2022. The average age of filed individuals is 29 years, which is also identical to 2022.

Of note, under 18 years was the only age group to record an increase (+43%, +425). Within this age group the largest increase was observed across those aged 16 years (+42%) and 17 years (+48%).

The relatively low volumes from a small number of members make it difficult to determine any meaningful judgement about a potential shift towards younger age groups at this stage.

Cases of misuse of facility increased by 5% (+3,261) in 2023

Those under 18 years recorded the largest increase in mule behaviour

Facility takeover

Cases of facility takeover increased by 13% compared to 2022, which is primarily attributed to a 59% rise in filings from the telecommunications sector (+6,431).

The online retail sector recorded the largest volume reduction but continues to be the second most impacted sector, accounting for 27% of cases (previously 38%).

The telecommunications sector is the most impacted for facility takeover filings, now accounting for 41% (previously 29%) of cases, following a spike in filings from several organisations. This increase partly reflects a shift in behaviour by criminals who are increasingly targeting mobile phone products for account takeover, compared to identity fraud in previous years.

A 59% rise in filings from the telecoms sector in 2023

The online retail sector accounts for 27% of cases filed

Criminals are targeting mobile phone products via account takeover

False application

In 2023, 19,840 false application cases were recorded to the NFD, representing a decrease of 17%.

This is primarily linked to a reduction across the bank account sector (-31%) which now accounts for 44% (previously 53%) of cases. Despite the overall reduction, there were increases across the loan (+25%), insurance (+20%), & telecoms sectors (+17%).

False documents recorded a 35% decrease, but this continues to be the dominant filing reason accounting for 30% (previously 39%). This reduction was spread across several sectors, but particularly bank accounts, with cases down 50% and fewer members recording this filing reason overall.

Falsifying proof of no claims rose 100% compared to 2022 (+878) and now accounts for 9% of cases when compared to 4% in 2022. This increase is attributed to several insurance members filing higher volumes in 2023.

False bank statements make up the largest proportion of filed documents (31%) followed by utility bills (28%).

19,840 false application cases recorded - a 17% decrease

Falsifying proof of no claims rose 100% from 2022

False bank statements make up largest proportion of filed documents

Insider Threat

A total of 325 individuals were recorded to the ITD (Insider Threat Database) in 2023 (up 14%, +41). In contrast to 2022, the most dominant case type recorded is now dishonest action to obtain benefit by theft or deception which now accounts for nearly half of cases (49%, previously 39%).

Feedback from Cifas member organisations indicates that this could be a result of financial pressures in light of the cost-of-living crisis.

The second most prominent case type is false employment application (unsuccessful) which accounts for 33% compared to 44% in 2022.

Overall, cases detected through internal controls have increased by 20% but continue to account for a similar proportion to last year (56%). This increase could be linked to organisations adopting greater monitoring/controls.

Most subjects engaged in dishonest conduct (38%) had been in their position for less than a year (previously 21%). This might be an early indication subjects are more willing to risk engaging in dishonest conduct in the early stages of employment. Alternatively, it could be linked to an uplift in more effective internal controls.

- 31% of those recorded for dishonest actions had been in employment for under one year, and 17% for over 10 years.
- 64% of those recorded for account misconduct had been in employment for less than one year.
- 80% of those recorded for bribery had been in employment for 10+ years.
- 75% of those recorded for unlawful obtaining or disclosure of commercial data have been in employment for less than five years

325 individuals recorded to the ITD in 2023 - up 14% from 2022

Dishonest action to obtain a benefit accounts for 49% of cases

Cases identified through internal controls increased by 20%

Summary & recomendations

In 2023, 374,160 cases were recorded to the NFD, representing a decrease of 9% compared to 2022. Despite this reduction, levels are still higher than 2021 by 4% (an increase of nearly 14,000 cases). The reduction in filed cases must be viewed in the context of the unprecedented volumes seen in 2022, but also as a result of some members within certain sectors enhancing their controls and tightening their criteria for new products and services throughout economic uncertainty.

Many organisations are concerned about the potential growth in AI generated fraud, enabling sophisticated phishing scams and synthetic identities.

Social media continues to offer threat actors numerous opportunities to access new victims or recruit dishonest individuals into fraudulent conduct.

Organisations also report continued social engineering of vulnerable consumers struggling with the cost-of-living crisis to divulge their personal data, allow access to their accounts, or authorise the payment of funds into fake investment schemes.

The challenges of the current economic uncertainty are driving some employees to dishonest conduct and this, combined with hybrid working, is making super vision more difficult. There are, however, positive signs that improved controls, a focus on wellbeing and staff awareness are mitigating these risks.

Changes in UK regulation and legislation in 2023 bring opportunities and challenges across the fraud prevention landscape. These include the Payment Systems Regulator's mandatory reimbursement requirements for Authorised Push Payment (APP) fraud, the Online Safety Act and the Economic Crime and Corporate Transparency Act 2023 (ECCTA). In addition, there are Bills in progress including the Data Protection and Digital Information Bill and the new Criminal Justice Bill which are likely to have an impact on counter-fraud efforts.

As the data in this report shows, the impact of fraud on individuals, businesses and the public sector has reached unprecedented levels. In order to drive down fraud we believe that action should be taken in five key areas:

- Provide cross-government leadership in the response to fraud, including through creating a Minister for Economic Crime.
- Improve the policing response to fraud through a ring-fenced fraud policing budget and by better harnessing the capabilities of the private sector to disrupt crime.
- Enhance support to victims of fraud, including business victims and victims of identity fraud.
- Modernise the criminal justice response to fraud, including through reviewing the law on identity theft.
- Ensure social media and online platforms are included in the multi-sector response to fraud, including by implementing the Online Safety Act Code of Conduct.

Cifas Commentaries

Overall

Market conditions and the tightening of controls and lending criteria due to economic uncertainty may be drivers behind the decline in filings in 2023. Although there was a reduction in filings, fraud continues to be the largest reported crime type to the police, now accounting for 40% of all crime[1].

Identity fraud continues to be the most dominant case type recorded to the National Fraud Database (NFD). It is also one of the most prominent types of fraudulent conduct in terms of impact and concern from surveyed Cifas member organisations[2]. Worries centred on social media enablers, the growing threat of AI and sophisticated data harvesting techniques designed to exploit an array of cost-of-living pressures. Issues of repeat victimisation and challenges in safeguarding customers who are more susceptible to ever-advancing social engineering tactics, especially where spoofing and brand impersonation are also deployed.

One in ten cases related to facility takeover, which saw the largest volume increase across all case types. Intelligence and Cifas data support a shift in tactics, with criminals increasingly targeting existing accounts to obtain new products or upgrades, particularly within the telecommunications sector. Threat actors continue to leverage phishing campaigns and the wealth of compromised data to take control of accounts directly, or to facilitate other frauds/scams.

Sophisticated attacks, for example credential stuffing, allow threat actors to target high volumes of accounts simultaneously, enabling criminal groups to quickly respond to rising demand for certain types of data such as online retail accounts.

Misuse of facility continues to be the second most dominant case type. A key driver is evasion of payment across several products. There was a reduction in cases that held intelligence indicative of money muling, however these cases still account for a large proportion of misuse of bank account filings. Social media appears to remain a key enabler to recruit young individuals, with other tactics such as employment scams becoming more prominent for harvesting data on prospective mules across other age groups.

Cases of false application fell overall, but there was an uplift against the loan, insurance and telecommunication sectors. False documents (usually bank statements and utility bills) are the dominant filing reasons, with individuals filed for providing false information or omitting details to obtain products and services.

Filings to the Insider Threat Database (ITD) increased in 2023. The rise in cases was driven by dishonest action by employees, with members reporting increasing financial pressures as a significant factor behind many cases. Theft of assets and non-return of high value devices was another key issue, exacerbated by the adoption of hybrid and remote working. Intelligence gaps centred on the true scale of polygamous working (particularly in the private sector) and the extent to which 'insider fraud as a service' threatens organisations.

1. ONS Reporting (April 2022-March 2023)
2. SIA Intelligence Requirement (2024-25)

Identity fraud

Higher quality falsified identity documents (particularly UK driving licenses) have been widely reported. In some cases, the same documents were being reused by different groups of perpetrators at high velocity. AI image generation and voice manipulation were reportedly being used to overcome biometric checks. Many commentators predict that the growing sophistication and ease of access to AI generated images will make detecting false identity documents increasingly challenging.

Organisations have reported that threat actors are also investing time in building fake identity profiles over extended periods to bypass Know Your Customer (KYC) checks. Social media remains a prominent platform for threat actors to advertise criminal services and recruit individuals. Access to recruitment at scale and the perception of a limited law enforcement response are assessed to be key factors, encouraging younger demographics to engage in this activity. Fraud tool kits[3] continue to be readily available, allowing novice threat actors to create fake websites, phishing campaigns and even AI assistants[4] to support their activity.

Sophisticated spoofing tactics and brand impersonation is a widespread theme, often impersonating genuine employees to harvest data on individuals and their logon/security credentials. Spoofed LinkedIn profiles, number spoofing and use of public registers have been cited as being abused to support convincing social engineering activity, particularly for corporate identity theft.

Facility takeover

Phishing remains one of the most dominant methods employed to take control of existing accounts. This is supported by global estimates suggesting 3.4 billion phishing emails are sent each day[5]. Threat actors continue to exploit the cost-of-living crisis to inform phishing and smishing campaigns, with recent examples centred on attractive mortgage rates[6] and scam employment opportunities. Once compromised, criminals can take control of victim accounts and build a more detailed picture of their lifestyle to facilitate further social engineering (often over longer periods).

Law enforcement has reported a high prevalence of rental fraud, ticket fraud and employment scams whereby data harvesting is a consistent theme. It is highly likely that these will remain key threats in 2024, potentially making greater use of AI to maximise their volume and impact. An emerging concern is audio fakes with organisations reporting voiceovers being used to answer security questions and circumvent voice authentication. Research suggests 56% of UK adults share their voice online at least once a week, giving cybercriminals enough to create a clone[7]. Intelligence has also highlighted growing concerns of dual pronged attacks specifically designed to harvest clips of victims' voices and their personal data.

Cifas data and intelligence sharing has demonstrated the scale of account takeover activity against certain sectors to obtain high value goods. The surge in online shopping and the value of data in this sector suggests it will continue to present an attractive target amongst criminal groups.

Organisations have reported that threat actors are increasingly aware of fraud controls and are changing tactics to circumvent these. Recent examples include fraudsters deliberately not changing personal details on compromised accounts to avoid detection.

3. Telekopye Telegram Bot Allows Cybercriminals' Phishing Scams (phishingtackle.com)
4. ChatGPT tool could be abused by scammers and hackers - BBC News
5. The Latest Phishing Statistics (updated April 2024) | AAG IT Support (aag-it.com)
6. Beware of fake mortgage lender emails | OPCC for Avon and Somerset (avonandsomerset-pcc.gov.uk)
7. Cifas – Deep Fake Technology Problem Profile 2023

Misuse of facility

Organisations continue to report applications submitted for loans, assets, and credit cards where there appears to be no intention of making payments. A common driver reported by multiple sectors is the continued cost-of-living pressure. Organisations noted challenges in predicting this activity, with some applicants demonstrating clean credit reports before facilities were subsequently misused.

Other prominent themes include individuals cancelling direct debit mandates immediately after inception, and false direct debit indemnity and charge back claims. This is further supported by the latest Cifas Fraud Behaviours Report which highlighted that 14% of UK adults have themselves, or know someone that has, falsely claimed they were a victim of impersonation on a loan product to avoid payment.

As 'Buy Now Pay Later' facilities grow in popularity, it is assessed that threat actors will increasingly look to abuse delayed credit facilities to dispute transactions on high value goods which can be sold for personal gain.

Cifas research[8] indicates that 20% of respondents believe that money muling is a reasonable activity, which is up from 16% in 2022. Of note, nearly one in five respondents believed money muling was also legal (18%).

Organisations continue to report the use of social media as a key enabler for promoting easy ways to make money or to harvest personal details of prospective mules. Threat actors are known to utilise algorithms to ensure their posts are viewed by as many as possible. Examples include a series of employment scams offering 'virtual PA' roles, where criminals impersonate financial institutions to advertise vacancies on genuine job listing sites. Successful applicants are socially engineered to divert funds or purchase 'gifts' for high value clients following a successful sale. Highly persuasive communications (including letters) were also received by victims, potentially enabled by generative AI platforms.

It is assessed that younger people who would typically gravitate towards other criminal activity might now be drawn into muling, believing it to be easier, with less risk and better profits. Money is earned directly, and they can upskill others over messaging groups, signalling an ever-evolving threat group. Students continue to be attractive targets for recruitment, including overseas students, where recent intelligence has highlighted high volumes of individuals selling their bank details before they leave the country.

8. Cifas Fraud Behaviours Survey 2023

False application

Organisations report that the rising cost-of-living and everyday expenses means there is greater temptation for individuals to provide false information or omit key details to obtain products and services. Common practices include falsifying pay slips to pass affordability checks and failing to disclose address histories, particularly when adverse credit is present.

The rising cost of insurance premiums is a likely driver behind the increase in filings for falsified no claims discounts[9]. Research suggests 33% of motorists have changed at least one material detail on their application to save money and 17% admit to insuring a car in their name, even if someone else is the main driver[10].

Findings from the Cifas Fraud Behaviours Report 2023 showed 9% of respondents felt it was reasonable to provide false information on a mortgage application, and 14% believed this to be legal, up from 13% in 2022. Those who believed this activity was reasonable tended to be aged 25-35 years, and those who believed this to be legal were typically aged between 45-54 years.

A primary enabler of false applications are the seemingly legitimate websites that offer fake bank statements, utility bills, and identity documents, which can then be used to support false applications. The increasing sophistication of false documents also poses a challenge, with some capable of bypassing verification checks.

Insider threat

Organisations reported the ongoing cost-of-living pressures, combined with remote working as a major contributor to the rise in cases. Reduced supervision is providing greater opportunity for staff to engage in dishonest conduct to supplement their income.

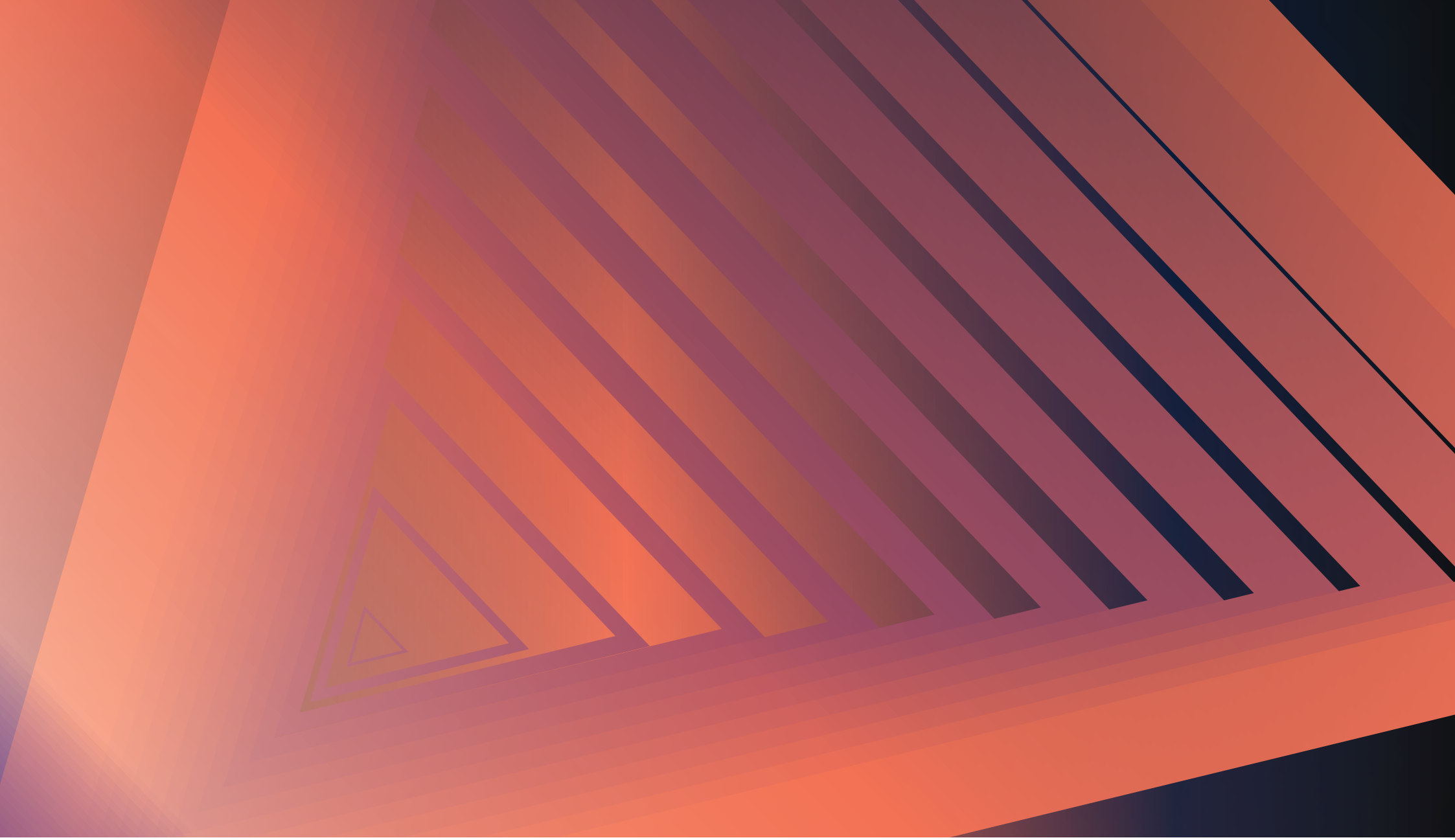
Polygamous working was one of the most prominent themes in 2023 with several organisations (particularly public sector) reporting this issue. It is assessed[11] that this practice is widespread in the private sector but remains a significant intelligence gap and challenge to detect. Of note, 1.2 million UK adults stated they had a second job[12] to cope with rising costs. Key concerns include employees contracting duties to third parties and theft of company/sensitive data to support new employment.

Theft of assets and non-return of high value devices is another consistent issue. Employees continue to exploit reduced face to face contact to steal devices for personal use, secondary jobs or to sell items via online marketplaces. This is particularly prominent with employees working abroad or project-based roles.

Organisations reported high levels of falsified CVs, as applicants compete for vacancies. Research shows one in 11 people in the UK have lied about their degree qualification in the last 12 months[13]. This issue has been exacerbated by the continued issues of 'reference houses' offering falsified references, bespoke career history and even fake KYC training courses to support their applications.

A growing concern is the potential for some employees to exploit their employee benefits to supplement their income. As employers broaden their benefit packages (sometimes with limited controls), there are increasing reports of online marketplace adverts where company loyalty programmes/discounts are offered for sale. These benefits offer real cash value and are increasingly attractive to criminal groups[14].

9. 'It's insane': motorists are driven to extremes by soaring insurance costs | Money | The Guardian
10. Aviva reports 16% rise in application fraud over same period in 2021 - Aviva plc
11. What can HR do about employees secretly working two jobs? (peoplemanagement.co.uk)
12. LFS: Workers with second jobs: UK: All: Thousands: SA - Office for National Statistics (ons.gov.uk)
13. Nearly a tenth of Brits admit they've lied on their CV in the last 12 months | Cifas
14. Cifas – Online Retail Threat Assessment 2023



cifas
Fighting Economic Crime Together

www.cifas.org.uk

6th Floor, Lynton House, 7-12 Tavistock Square
Bloomsbury, London WC1H 9LT

Version - 08/04/2024