cifas
Fighting Economic Crime Together

FRAUDSCAPE 2026

WWW.FRAUDSCAPE.CO.UK

Fighting Fraud and Financial Crime Together

Protecting organisations and individuals from fraud and financial crime through the sharing of data, intelligence, and learning.


Data


Intelligence


Learning

CONTENTS

1. INTRODUCTION

Welcome to Fraudscape 2026

It provides a comprehensive assessment of fraud risk in the UK, drawing on data filed by Cifas members to the National Fraud Database (NFD) and Insider Threat Database (ITD) in the 12 months to December 2025, alongside intelligence from members, partners and law enforcement

Taken together, the data from these sources present a clear and compelling picture of the scale, complexity and evolving nature of the fraud threat. They highlight both the pressures facing the fraud prevention community today and the emerging threat vectors that demand sustained focus and collective action.

The headlines are sobering. In 2025, a record 444,993 cases were filed to the NFD, including more than 242,000 cases of identity fraud. Although identity fraud filings fell by 3% year-on-year, it is still the most common case type, accounting for over half of all reports. This modest reduction is accounted for by a shift in criminal tactics rather than a reduction in harm, with fraudsters increasingly targeting account takeovers, particularly via mobile phones.

1. Crime in England and Wales: year ending June 2025.
2. Annual Fraud Indicator
3. 9.4billion_stolenfromconsumers

The threat from fraud is also global and organised, with criminal gangs now mimicking the size and structures of large corporations. Scam factories in West Africa and South-East Asia house thousands of enslaved workers in appalling conditions, criminalising the vulnerable and economically insecure, forcing them to build and operate a sophisticated infrastructure of call centres and websites intended for the sole purpose of stealing people's money.

Fraud now accounts for almost 44%[1] of all crime reported in England and Wales and is estimated to cost the UK economy £219 billion[2] each year, including up to £81 billion in losses to the public sector. Consumers lost £9.4 billion[3] to scams in 2024 alone, with those aged 61 and over remaining most at risk of identity fraud and account takeover.

Fraud is also increasingly digital. Four in five scams are now digitally enabled, with criminals moving seamlessly across platforms, services and technologies. It is global and highly organised, with networks operating at scale and exploiting both technology and human vulnerability.

Our assessment suggests that online fraud will become ever more sophisticated, supercharged by AI-powered impersonation, synthetic media, and accessible fraud-as-a-service tools that are likely to ensure that identity fraud and account takeover remain major threats.

Synthetic identities are becoming industrialised, with criminals building convincing long-term profiles that blur the lines between real users and AI-generated imposters. At the same time, more individuals are selling or sharing their identity documents under financial strain, creating increased opportunities for misuse.

While this year's Fraudscape report shows that progress is being made, it also underlines the scale of the challenge that remains. Through the use of Cifas' products and services, our members prevented more than £2.4 billion in fraud losses last year. But no organisation can tackle fraud alone. It is only through effective collaboration and the sharing of data and intelligence that we can stay ahead of increasingly sophisticated criminals. This is why Cifas exists.

We hope this report provides valuable insight into the evolving fraud landscape. By working together, I hope we can use this report as the catalyst for action, to strengthen defences, deepen collaboration and collectively take the fight to the criminals.

2 OVERVIEW

SECTOR	2024	2025	VOLUME CHANGE	% CHANGE	PROPORTION 2024	PROPORTION 2025
ASSET CONVERSION	731	709	-22	-3%	0%	0%
FALSE APPLICATION	21,585	16,431	-5,154	-24%	5%	4%
FALSE INSURANCE CLAIM	644	966	322	50%	0%	0%
FACILITY TAKEOVER	74,259	78,387	4,128	6%	18%	18%
IDENTITY FRAUD	249,430	242,003	-7,427	-3%	59%	54%
MISUSE OF FACILITY	74,352	106,497	32,145	43%	18%	24%
TOTAL	421,001	444,993	23,992	6%	-	-

444,993 CASES FILED

+6% INCREASE FROM 2024

RECORD LEVELS OF ACCOUNT TAKEOVERS AND BANK ACCOUNT MISUSE DRIVE GROWTH

In 2025, over 444,000 cases were filed to the National Fraud Database. This is a record number of cases (+6%) and continues the upward trend seen in 2024

Identity fraud continues to account for the largest share of cases, representing 54% of all filings, followed by misuse of facility at 24% and facility takeover at 18%. Together these are the driving forces behind the latest overall rise, with particularly high levels of account takeovers against telco products and the growing misuse of bank accounts.

3

IDENTITY FRAUD

242,003
IDENTITY FRAUD CASES

-3%
DECREASE FROM 2024

LEVELS OF IDENTITY FRAUD DIP

In 2025, 242,003 cases of identity fraud were recorded

Identity fraud fell by 3% compared to 2024, with the largest drop in cases seen in the telecoms sector (-24%).

However, this decline reflects a shift in criminal tactics rather than a genuine reduction in harm, as threat actors increasingly move towards account takeovers, particularly targeting mobile phone accounts. Despite the decrease, identity fraud is the most common filed case type, making up 54% of all NFD filings.

Although identity fraud fell overall, five sectors reported increases compared with 2024. The biggest rises were in bank accounts (+5,372 cases, +10%) and insurance (+3,355 cases, +26%). Within banking, personal instant and easy-access accounts saw a dramatic 455% rise (+7,131 cases), suggesting threat actors are shifting towards the targeting of basic banking products using stolen or synthetic identities. In insurance, increases continue to be driven by motor insurance, which is up 26% year-on-year.

Plastic cards remain the most affected sector, accounting for 36% of all identity fraud. Personal credit cards are overwhelmingly the main target of these, representing 92% of filings. Communications and online retail are also significant, together making up 33% of all identity fraud cases.

Victims of impersonation are older with those over 61 most commonly targeted. Filings in relation to this age group rising by 13%, representing 29% of all cases. Those aged 51–60 follow at 21%. Identity fraud involving victims under 21 increased by 8%, linked to the greater willingness among younger people to share personal information online.

Our assessment indicates that online fraud will continue to become more sophisticated, supercharged by AI-powered impersonation, synthetic media, and accessible fraud-as-a-service tools that are likely to ensure identity fraud and account takeover remain major threats.

The use of synthetic identities is becoming industrialised, with criminals building convincing long-term profiles that blur the lines between real users and AI-generated imposters. At the same time, more individuals are selling or sharing their identity documents under financial strain, creating increased opportunities for misuse.

IDENTITY FRAUD CASES

SECTOR	2024	2025	VOLUME CHANGE	% CHANGE	PROPORTION 2024	PROPORTION 2025
ALL IN ONE	58	72	14	24%	0%	0%
ASSET FINANCE	1,558	1,236	-322	-21%	1%	1%
BANK ACCOUNT	57,946	63,678	5,732	10%	23%	26%
COMMUNICATIONS	36,452	27,659	-8,793	-24%	15%	11%
INSURANCE	13,106	16,461	3,355	26%	5%	7%
LOANS	15,635	14,220	-1,415	-9%	6%	6%
MORTGAGE	30	43	13	43%	0%	0%
ONLINE RETAIL	18,581	17,794	-787	-4%	7%	7%
OTHER	11,944	13,022	1,078	9%	5%	5%
PLASTIC CARD	94,120	87,818	-6,302	-7%	38%	36%
TOTAL	249,430	242,003	-7,427	-3%	-	-

4

ACCOUNT TAKEOVER

78,387
ACCOUNT TAKEOVER CASES

18%
OF NFD FILINGS

ACCOUNT TAKEOVER SURGES

Over 78,000 account (facility) takeover cases were reported in 2025, a rise of 6% compared to 2024

This has been driven primarily by a significant increase in filings from the telecommunications sector (+38%). Cases linked to mobile phone products dominate, followed by online retail and personal credit cards.

Collectively, these products account for 90% of all account takeover filings. Nearly 1 in 5 (18%) of all fraud-risk cases reported to the NFD are now account takeovers.

The telecommunications sector recorded the greatest volume of account takeover cases. It now accounts for the majority of such cases (62%, previously 48%), driven by the sustained rise in mobile phone-related filings.

The leading filing reason for account takeover in 2025 was 'unauthorised addition of facility' and 'unauthorised security/personal details change', with filings predominantly relating to mobile phones, online retail, and personal credit cards.

There has been a notable rise in unauthorised SIM swaps (+38%). This increase appears to be driven by the growing availability of stolen personal data, and the use of more automated methods for compromising accounts.

Victims aged 61 and above are the most frequently targeted age range, accounting for 31% of cases, with filings in relation to this age group up 10% compared with 2024.

Criminals are exploiting AI to enhance malicious communications and automate large-scale credential attacks, contributing to the rising threat of takeovers. Techniques such as hyper-personalised scams, deepfake audio targeting call centres and SIM hijacking are becoming more prevalent, enabling attackers to bypass authentication processes and mimic legitimate login behaviour, making unauthorised access harder to detect.

As methods become more advanced, SIM swap attacks are expected to continue rising, fuelled by widespread reliance on mobile-based authentication.

Account takeovers are also becoming more integrated into multichannel operations, where criminals combine and enrich stolen data to maximise impact and financial return. As organisations strengthen their defences, attackers are increasingly focusing on stealth – disabling customer alerts, flooding inboxes, spoofing devices, and slowly altering profile details to blend malicious behaviour with normal user activity.

ACCOUNT TAKEOVER CASES

SECTOR	2024	2025	VOLUME CHANGE	% CHANGE	PROPORTION 2024	PROPORTION 2025
ALL IN ONE	2,029	756	-1,273	-63%	3%	1%
ASSET FINANCE	32	15	-17	-53%	0%	0%
BANK ACCOUNT	4,735	4,250	-485	-10%	6%	5%
COMMUNICATIONS	35,415	48,805	13,390	38%	48%	62%
INSURANCE	25	40	15	60%	0%	0%
LOANS	486	1,438	952	196%	1%	2%
MORTGAGE	4	1	-3	-75%	0%	0%
ONLINE RETAIL	19,921	14,026	-5,895	-30%	27%	18%
OTHER	238	442	204	86%	0%	1%
PLASTIC CARD	11,374	8,614	-2,760	-24%	15%	11%
TOTAL	74,259	78,387	4,128	6%	-	-

5

MISUSE OF FACILITY

106,497
MISUSE OF FACILITY CASES

+43%
INCREASE FROM 2024

LEVELS OF MISUSE INCREASE

In 2025, over 106,000 cases of misuse of facility were recorded to the NFD – a 43% increase on 2024

Of the members that filed in both 2024 and 2025, 54% observed a rise. The majority of these filings involve significant incidents of bank account misuse.

The bank account sector continues to be the main source of misuse filings (82% of cases), rising 44% in 2025 - driven largely by a 35% increase in filings in relation to personal current accounts.

Payment fraud is now the largest category in this sector, accounting for 31% of filings, up from 20% in 2024.

Increasing bank account misuse reflects the evolving recruitment tactics of fraudsters, with victims encouraged to pass on funds or share banking details. In some cases, personal information is being sold to criminal networks to support account opening and misuse.

Overall, payment fraud rose 239% during 2025 and now makes up 40% of all misuse filings, mainly driven by personal current accounts and credit cards.

Evasion of payment is also up 22%, linked to high volumes of loan, asset, and credit card applications with no intent to repay.

Additionally, misuse cases in the communications (which includes telecoms sector) rose 106% in 2025, mainly due to mobile phone filings linked to evasion of payment. Although driven by a small number of members, this may signal a shift towards customers avoiding payment for everyday items.

Cifas' research points to an increasing societal acceptance[4] of first-party fraud, this is reflected in member data which also shows increases in both payment evasion and broader account misuse.Misuse of personal money transfer accounts also increased +43%, suggesting criminals are expanding into other account types to avoid detection.

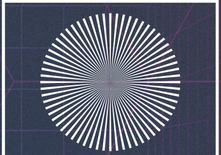
4. Cifas Fraud Behaviours Survey 2024

MISUSE OF FACILITY CASES

SECTOR	2024	2025	VOLUME CHANGE	% CHANGE	PROPORTION 2024	PROPORTION 2025
ALL IN ONE	279	243	-36	-13%	0%	0%
ASSET FINANCE	1,594	1,691	97	6%	2%	2%
BANK ACCOUNT	60,753	87,554	26,801	44%	82%	82%
COMMUNICATIONS	1,423	2,932	1,509	106%	2%	3%
CREDIT FILE/ IDENTITY SERVICES	3	0	-3	-100%	0%	0%
INSURANCE	27	24	-3	-11%	0%	0%
LOANS	5,012	4,172	-840	-17%	7%	4%
MORTGAGE	15	6	-9	-60%	0%	0%
ONLINE RETAIL	119	362	243	204%	0%	0%
OTHER	671	3,304	2,633	392%	1%	3%
PLASTIC CARD	4,214	6,099	1,885	45%	6%	6%
PUBLIC SECTOR SERVICES	242	110	-132	-55%	0%	0%
TOTAL	74,352	106,497	32,145	43%	-	-

6

MONEY MULES



22,000 CASES USING NEW FILING TYPE

89% OF FILINGS INVOLVE A BANK ACCOUNT

NEW MULES CATEGORY SHINES A LIGHT ON THE THREAT

In 2025, more than 22,000 incidents of money muling were reported to the NFD, following the introduction of a new money mule filing category

Cases primarily involved personal bank accounts, which accounted for 89% of money muling filings, as well as business bank accounts, which comprised 4% in 2025. This newly introduced Cifas filing category now enables muling activity to be more reliably tracked across an expanding range of facilities, such as personal credit cards, pre-paid cards and money transfer accounts.

The rising misuse of bank accounts reflects some of the many ways individuals receive fraudulent funds or give away their banking details.

Intelligence indicates that some people are actively selling their personal information to criminal networks, allowing them to construct credit profiles using some or all of that data and open accounts for illicit use.

Concerningly, 35% of Gen-Zs surveyed by Cifas have said they would transfer money to a stranger for a fee.[5] Although this group poses a risk, a high proportion of offboarded customers are aged 30-39, with increases also seen in those aged under 16, highlighting the need for impactful messaging to all. Separately, Cifas research[6] also shows a fifth of individuals don't believe that money muling is illegal, highlighting a lack of knowledge and understanding of the significant risks involved.

Intelligence from Cifas members highlights muling as a persistent threat, with diverse recruitment tactics ranging from job scams to customers receiving over-payments when selling items via online marketplaces. Social media is a key channel for luring new mules and advertising 'quick money' schemes. Although greater awareness might lead to criminals changing fraudulent techniques, recruitment tactics are predicted to remain focused on mimicking employment or business opportunities.

5. Cifas Fraud Behaviours Survey 2024
6. Cifas Fraud Behaviours Survey 2024

MONEY MULE AGE RANGE

AGE RANGE	PROPORTION %
UNDER 21	18%
21-30	39%
31-40	23%
41-50	12%
51-60	5%
61+	2%

7

FALSE APPLICATION

16,431
FALSE APP CASES FILED IN 2025

24%
DECREASE IN FILINGS FROM 2024

FALSE APP LEVELS COLLAPSE

Over 16,000 cases of false application were recorded to the National Fraud Database in 2025, a 24% fall on 2024

Reductions were observed across many sectors, with the largest decline in relation to bank account cases (-27%). Among those Cifas members who submitted cases in both 2024 and 2025, the majority (55%) reported a decrease.

Filings continue to be concentrated in motor insurance and personal bank accounts, which together account for 62% of all cases.

In 2025, 65% of false applications were received through online channels, down from 80% in 2024. This reduction is mainly due to a rise in false mobile app applications. The trend indicates a shift towards app-based application methods, particularly in banking.

The bank account sector was the largest source of false applications (38% in 2025), though numbers have still fallen. Undisclosed adverse addresses were the most common filing reason, accounting for 46% of cases (up from 40%). In contrast, false document filings for personal current accounts decreased by 41%, reflecting reports from members around improved controls and greater investment in fraud detection tools.

The insurance sector recorded a 30% drop in filings, following unusually high volumes in 2024. This was mostly driven by the reporting of fewer cases from a small number of members.

Members reported that false applications are still a major concern. Although often seen as a 'victimless' crime, first-party frauds such as these are becoming more common, contributing to rising prices and premiums. Independent Cifas research also shows a growing social acceptance of this behaviour.[7] An example of this is the increase in filings relating to tenant referencing which increased by 263% driven by false and altered documents.

Those aged 25–34 are most likely to engage in first-party fraud,[8] with behaviour driven by cost-of-living pressures, uncertainty at what constitutes fraud, and greater exposure to advertising and malicious content offering unrealistically attractive deals and rates.

Cifas members also reported widespread income and affordability manipulation, supported by realistic fake document websites. Risks are further heightened by AI-enabled document forgery and unregulated brokers posing as 'application helpers', with some fake documents reused repeatedly across multiple applications.

7 Cifas Fraud Behaviours Survey 2024
8 Cifas Fraud Behaviours Survey 2024

FALSE APPLICATION CASES

SECTOR	2024	2025	VOLUME CHANGE	% CHANGE	PROPORTION 2024	PROPORTION 2025
ALL IN ONE	40	2	-38	-95%	0%	0%
ASSET FINANCE	2,029	1,543	-486	-24%	9%	9%
BANK ACCOUNT	8,615	6,313	-2,302	-27%	40%	38%
COMMUNICATIONS	1,022	354	-668	-65%	5%	2%
CREDIT FILE/ IDENTITY SERVICES	8	2	-6	-75%	0%	0%
INSURANCE	5,590	3,932	-1,658	-30%	26%	24%
LOANS	1,900	1,442	-458	-24%	9%	9%
MORTGAGE	1,594	1,397	-197	-12%	7%	9%
ONLINE RETAIL	15	12	-3	-20%	0%	0%
OTHER	475	1,112	637	134%	2%	7%
PLASTIC CARD	155	207	52	34%	1%	1%
PUBLIC SECTOR SERVICES	142	115	-27	-19%	1%	1%
TOTAL	21,585	16,431	-5,154	-24%	-	-

8

INSIDER THREAT

288
INSIDER THREAT CASES FILED

21%
INCREASE IN FILINGS FROM 2024

INSIDER THREAT CASES RISE

In 2025, 288 subjects were filed to the Insider Threat Database (ITD) – a 21% increase on 2024

'Dishonest action by staff to obtain a benefit by theft or deception' is the most common case type and again accounts for the largest share of filings made to the ITD. Volumes increased by 28%, rising from 116 to 148. It now accounts for 48% of all cases.

The most frequent filing reasons were abuse of company time or privilege (15%), false expenses submissions (13%), and theft of IT equipment (11%).

Internal controls and audits uncovered 45% of dishonest behaviour, with staff reporting responsible for a further 21%, highlighting the critical role of employee awareness and speak-up cultures.

'False employment application – unsuccessful' was the next highest volume and saw a notable increase on 2024 (+25%). As fraudulent job applications continue to rise, this underscores the need for strong pre-employment screening to stop unsuitable or high-risk individuals entering organisations.

The most common issues were hidden adverse credit history (40%), followed by concealed employment history (20%) and concealed employment records (15%). Although formal filings remained steady, intelligence reports on false references increased, often driven by reference houses selling fake work histories or training certificates - allowing candidates to bypass vetting and gain access to sensitive data.

Internal controls and audits uncovered 45% of dishonest behaviour, with staff reporting responsible for a further 21%, highlighting the critical role of employee awareness and speak-up cultures.

Employees are also seeking to supplement income through a wide range of dishonest methods. This is reflected in more than 24 categories of filings – from inflated expenses to manipulation of reward schemes. As some organisations broaden staff benefits with only limited controls, there is a high likelihood these perks – such as staff discounts or loyalty rewards – will be exploited or resold for financial gain.

Online insider approaches, often disguised as legitimate networking on platforms like LinkedIn, are a growing blind spot for organisations. Those holding large volumes of personal data, including telecoms and banks, may be particularly exposed.

INSIDER THREAT CASES

SECTOR	2024	2025	VOLUME CHANGE	% CHANGE	PROPORTION 2024	PROPORTION 2025
ACCOUNT MISCONDUCT	23	22	-1	-4%	9%	7%
DISHONEST ACTION BY STAFF TO OBTAIN A BENEFIT BY THEFT OR DECEPTION	116	148	32	28%	46%	48%
FALSE EMPLOYMENT APPLICATION (SUCCESSFUL)	20	17	-3	-15%	8%	5%
FALSE EMPLOYMENT APPLICATION (UNSUCCESSFUL)	77	96	19	25%	30%	31%
UNLAWFUL OBTAINING OR DISCLOSURE OF COMMERCIAL DATA	3	5	2	67%	1%	2%
UNLAWFUL OBTAINING OR DISCLOSURE OF PERSONAL DATA	15	17	2	13%	6%	5%
BEING BRIBED	0	3	3	-	-	1%
BRIBING ANOTHER PERSON	0	2	2	-	-	1%
TOTAL	254	310	56	22%	-	-

A subject in an individual ITD case can be counted in multiple types of dishonest conduct which is reflected in the numbers on this table.

WWW.FRAUDSCAPE.CO.UK

cifas
Fighting Economic Crime Together

www.cifas.org.uk

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

Version -09.03.2026