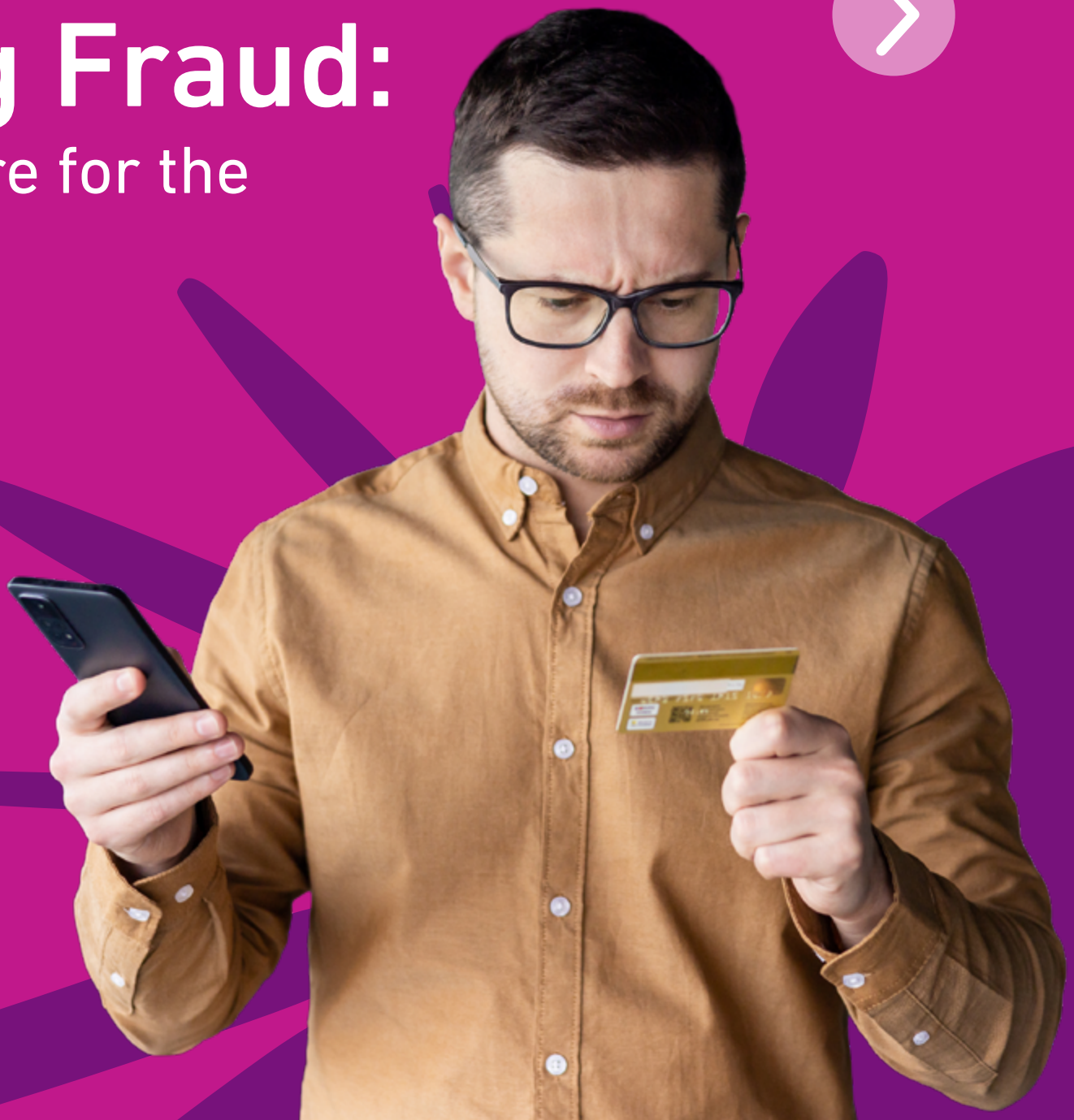
Unwrapping Fraud:

Helping you to prepare for the festive season ahead



experian | cifas

Fighting Economic Crime Together

Preparation is key for a stress-free festive season

Everyone wants to switch off and relax over the holidays. But for businesses, the increased risk of fraud means you must stay vigilant.

As spending surges across November, December and January, so too do instances of identity theft, facility takeover, refund abuse and holiday-related scams. A rise in instore and online traffic puts more strain on fraud controls and makes it harder for operations teams, employees and temporary seasonal staff to spot suspicious activity. The result is a 'perfect storm' for fraudulent behaviour to flourish.

Fraudsters know this and use a range of techniques to try and exploit businesses, consumers and employees. New methods are constantly emerging, with deepfake messages becoming increasingly common alongside the more established delivery or eCard scams.

This report combines Experian's analytical insights with intelligence drawn from the Cifas National Fraud Database. Together, we set out to map the key fraud threats businesses face during the festive season, highlight emerging trends and offer practical steps organisations can take to protect themselves and their customers.

Foreword from Paul Weathersby, Chief Product Officer, Identity and Fraud at Experian UK&I

As we approach the festive season – a time of celebration and heightened consumer activity – it is vital to acknowledge a growing and concerning reality. Fraud is surging across the UK, and neither businesses nor consumers are immune.

This new report offers an urgent examination of the evolving fraud landscape, revealing how technology is both a threat and a powerful tool in the fight against financial crime.

Experian alone has prevented more than £10.7bn in fraudulent applications over the last five years. Our new analysis, produced for the report, reveals the scale of the challenge we face. Identity fraud – when someone's personal information is used without their consent to apply for financial products, such as credit cards and loans – has risen by 9.2% in the last three years, with synthetic fraud/AI generated identities now making up 42% of all cases.

Identity fraud, when someone's personal information is used without their consent to apply for financial products, such as credit cards and loans has risen by 9.2% in the last three years, with synthetic fraud/AI generated identities now making up 42% of all cases.

The rise of AI-enabled fraud is one of the most pressing threats facing businesses today. Fraudsters are leveraging generative AI to craft convincing phishing emails, deepfake communications and synthetic identities that bypass traditional security measures.

Foreword from Paul Weathersby, Chief Product Officer, Identity and Fraud at Experian UK&I

But AI is not only part of the problem; it's also part of the solution. Businesses are increasingly deploying AI-driven tools to detect anomalies, verify identities and monitor for suspicious behaviour in real time. Multi-layered verification systems, behavioural analytics and biometric checks are helping organisations stay one step ahead of fraudsters.

This report also explores the seasonal spike in fraud, particularly in Q4, where card fraud, facility takeovers and online shopping scams rise sharply. The festive period presents unique vulnerabilities, with consumers more likely to fall for fake deals, spoofed websites and phishing campaigns disguised as delivery notifications or eCards.

As fraudsters become more sophisticated, collaboration and intelligence-sharing are essential. By working together, businesses can strengthen defences, educate their staff and protect customers. Experian and Cifas remain committed to supporting organisations with data, insights and tools to combat fraud smarter and faster.

We hope this report serves as a wake-up call for action. The threat is real, but so is our ability to fight back with vigilance, innovation and collective resolve.

Paul Weathersby,
Chief Product Officer,
Identity & Fraud

Foreword from Mike Haley, CEO at Cifas

As the festive season draws near, many of us are looking forward to winding down, spending time with loved ones, and enjoying the spirit of giving. But while households and businesses prepare to relax, criminals are gearing up for one of their busiest times of the year.

Fraudsters don't take a holiday. In fact, many thrive during periods of increased spending, stretched resources, and seasonal staffing – creating a 'perfect storm' for them to thrive.

Official estimates show fraud is rising 14% year-on-year with well over £200 billion stolen from the UK economy annually. In the last 12 months, scammers took a staggering £9.4 billion, with victims having £878.60 stolen on average, each time. These figures are more than statistics, they represent real people and businesses impacted by deception and criminal exploitation.

We have seen these figures reflected in our own data and intelligence at Cifas too. In 2024, there were record levels of cases filed to the National Fraud Database – a rise of 13% compared to 2023, with over 421,000 reported cases. Our data for the first half of 2025 suggests this record will be surpassed again.

There's no question fraud has been supercharged by the use of generative AI. Deepfakes, synthetic identities, and real-time manipulation of biometric systems are all lowering the barriers to entry for fraudsters and increasing the emotional and financial toll on victims.

Foreword from Mike Haley, CEO at Cifas

Fraud may be evolving, but so is our response. The policy landscape is shifting, with the UK appointing its first dedicated Minister for Fraud, Lord Hanson, and a new national strategy on the horizon. Collaboration between industry and law enforcement is strengthening, with data and intelligence sharing helping to detect and prevent more fraud and scams, in turn protecting more consumers. Meanwhile, businesses are harnessing AI to accelerate prevention and detection – turning technology into a powerful ally in the fight against fraud.

You'll see important insights throughout this joint report designed to help organisations prepare for the seasonal surge in fraud. It combines Experian's analytical expertise with data and intelligence from Cifas to map out the key threats businesses face. From rising identity fraud – a £1.8 billion problem – to refund abuse and account takeovers, new and more sophisticated techniques are challenging organisations to evolve their approach to fraud prevention. We also offer actionable advice to help companies keep their customers safe from the significant harm fraud can cause.

We hope you enjoy this report and join us in our collaborative efforts to stop fraud at the source. Only by sharing cross-sector data and intelligence, can we collectively build a more protected and resilient society, ensuring the festive season remains a time of joy for all.

Mike Haley,
Chief Executive Officer
Cifas

Fraud doesn't take holidays

The period between Black Friday and the end of the January sales is traditionally very busy for UK retailers and service providers. Although this has dipped slightly in recent years, the end of 2025 is still likely to see a rise in online and in-store activity.

While the surge is a critical contributor to annual revenue, it also gives fraudsters more opportunities to slip past defences.

During this period, retailers, ecommerce, warehousing and logistics companies often operate at full stretch. Longer trading hours, temporary seasonal staff and high volumes of orders all combine to weaken the usual checks and increase the chance of human error. At the same time, shoppers are more likely to rush through purchase processes to get better deals or make sure products are delivered in time. This makes them more susceptible to 'too good to miss' deals or clicking on links disguised as delivery updates.

Taken together, these seasonal changes in both business and consumer behaviour open the door to oversight as well as more malicious policy abuse, chargeback fraud and account takeovers. Fraudsters exploit this softer environment, timing actions to coincide with predictable spikes in demand. Using phishing emails, social media impersonation and increasingly sophisticated synthetic identities, they can blend in with genuine activity, striking when businesses are least able to respond.

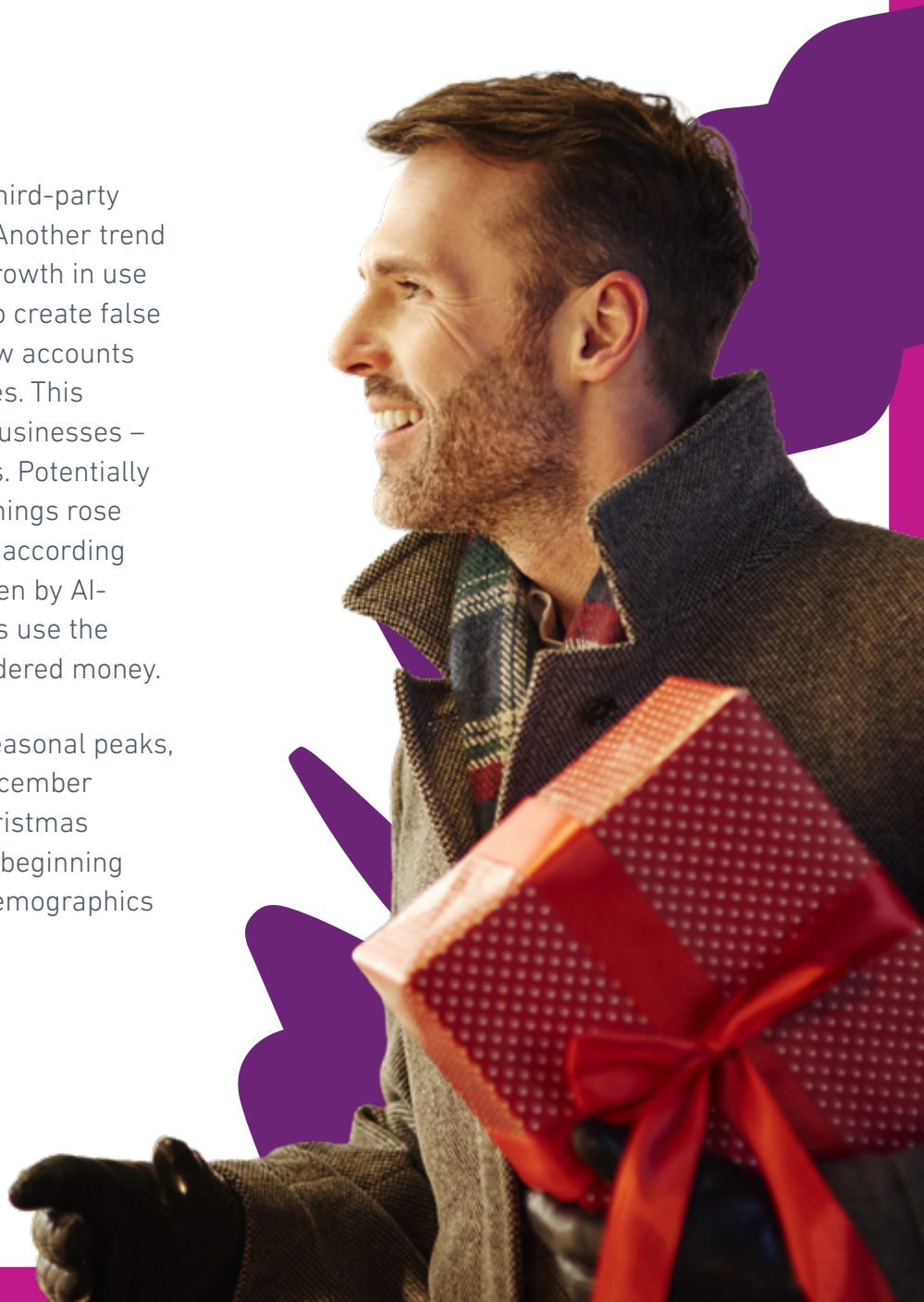
Technological evolution is also creating a simultaneous arms race between businesses and fraudsters. On one hand, fraudsters are increasingly using AI-powered tools to generate hyper-realistic deepfakes and automate attacks. These fresh techniques are likely to be deployed at scale during the 2025 holiday season. At the same time, companies are leveraging advanced tools like AI and layered identity checks to build smarter, adaptive security defences that catch complex scams, like synthetic IDs and account takeovers, in real-time.

Fraud trends for 2025

The unprecedented rise in fraud over the last couple of years in the UK is an emergency that needs to be tackled as a national priority. In the first six months of 2025, Cifas members recorded over 217,000 fraud-risk cases to the National Fraud Database – the highest number for a six-month period ever.

Third-party fraud dominates across all products in the last three months of the year. Identity fraud continues to rise year-on-year, with data from Fraudscape showing a 76% increase in facility takeover fraud. This kind of fraud now represents 18% of all Cifas National Fraud Database filings, with application fraud making up 5%. Experian data also shows a 9.2% rise in third-party fraud over the last three years. Another trend highlighted by Experian is the growth in use of AI and deepfake technology to create false and synthetic identities. This now accounts for 42% of all identity fraud cases. This represents a big challenge for businesses – particularly financial institutions. Potentially fraudulent savings account openings rose by 53% during the same period, according to Experian, with much of it driven by AI-generated identities as criminals use the account to house stolen or laundered money.

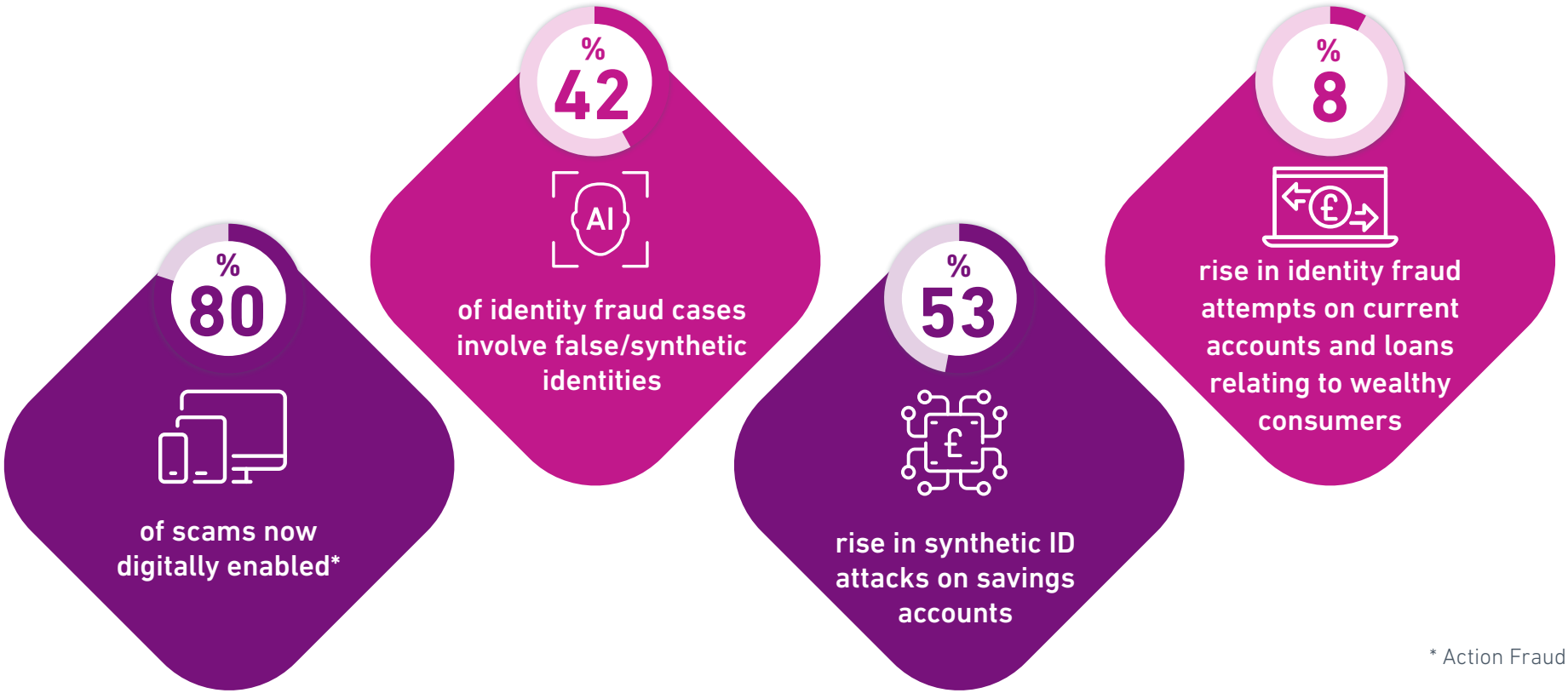
Card fraud shows predictable seasonal peaks, spiking every November and December in line with Black Friday and Christmas spending. However, we are also beginning to see patterns in the specific demographics that are being targeted.



The data shows that 'Money Makers' and 'Growth Phase' consumers (aspirational and relatively wealthy individuals) are most exposed to third-party fraud. Experian's data shows that identity fraud attempts on this group's current accounts and loans have seen an 8% increase.

These figures show that the scale of fraud is worsening and illustrate why businesses need to get prepared for the holiday season. The challenge for 2025 will be to close the gap between the pace of criminal innovation and the speed of business and law enforcement response. This makes collaboration and data sharing among organisations like Experian and Cifas, as well as the continued implementation of advanced detection tools by businesses, more important than ever.

Fraud in 2025 – at a glance



* Action Fraud 2025

The three 'high growth' frauds that could dominate the 2025 holiday season

While it is impossible to predict exactly what shape holiday fraud will take this year, the data is showing some clear patterns in behaviour. Based on cases filed to the Cifas National Fraud database over the last three years, we anticipate that three types of fraud will grow fastest over the next 12 months:

Facility (account) takeover

Identity fraud

False application fraud

1 Facility (account) takeover

Cases surged from **42,091** in 2023 to **74,256** in 2024 (**+76%**)

The telecoms sector alone saw a **105%** rise in account takeover fraud in 2024, with SIM swap fraud growing **1,055%**

Online retail also saw a **75%** increase in account takeovers

New insights from Experian reveal over a third (**35%**) of UK businesses reported being targeted by AI-related fraud in the first quarter of 2025, compared to just **23%** last year.

2 Identity fraud

Fraudscape data shows that between January and July 2025, there were **118,726** cases of identity fraud filed – accounting for **55%** of all cases recorded to the National Fraud Database

Cases rose from **237,682** in 2023 to **249,417** in 2024 (**+5%**)

86% of identity frauds now occur online, with telecoms showing a **73%** rise in impersonation. AI-generated documents and deepfakes are fuelling growth, with older adults again being the most affected group

3 False application fraud

Cases grew from **19,820** in 2023 to **21,708** in 2024 (**+10%**)

80% of cases are now online – compared to **73%** in 2023

Economic pressures are leading to a rising social acceptance of this kind of fraud, with **48%** of UK adults believing some first-party fraud is 'reasonable' (Cifas' independent 'Fraud Behaviours Survey' research)

Insurance filings rose **89%** (notably false 'no claims discount' up **86%**), while communications filings increased **69%**

Together, these three fraud types show how AI, digital channels and social acceptance of fraud are converging to change the risks businesses face during the last three months of 2025.

The eight frauds of Christmas

As the festive season hits full volume, fraudsters cue up their 'festive favourites' on repeat. There are the old classics that get played every year like refund abuse, mule recruitment and social media scams. But lately, the playlist has expanded to include a range of new hits – AI-powered deepfakes, crypto scams and SIM swap fraud.

1

AI-powered scams and deepfakes

What is it?

Fraudsters use generative AI to create convincing phishing emails, cloned voices or even deepfake video calls to trick businesses and employees.

How does it work?

AI can automate scam content at scale, test variations until one succeeds and impersonate trusted figures to bypass scepticism.

Why does it spike at Christmas?

The festive season is often characterised by increased financial pressure, high volumes of online shopping and delivery notifications, and a general atmosphere of greater goodwill that lowers people's guard. Fraudsters leverage the extended gap between paydays and the urgency of gift-buying to trick individuals into falling for scams, particularly those faking delivery updates.

New insights from Experian reveal over a third (**35%**) of UK businesses reported being targeted by AI-related fraud in the first quarter of 2025, compared to just **23%** last year.

2

Identity fraud (third-party)

What is it?

Criminals use stolen or synthetic personal details to open financial products or gain access to services in someone else's name.

How does it work?

Fraudsters exploit gaps in onboarding processes, often using false documents or fabricated digital identities created using AI to pass checks.

Why does it spike at Christmas?

High demand for credit cards, loans and retail finance in Q4 creates opportunities for fraudsters to blend in with high volumes of genuine applicants.

Identity fraud is estimated to cost the UK economy £1.8bn a year (Cifas & RUSI)

The eight frauds of Christmas

3

Account takeover

What is it?

Criminals gain access to existing customer or employee accounts and use them for fraudulent transactions or data theft.

How does it work?

Phishing, credential stuffing and intercepted delivery details allow fraudsters to hijack accounts.

Why does it spike at Christmas?

Increased online shopping and frequent delivery tracking give fraudsters more chances to lure victims with phishing and smishing attacks.

Facility takeover fraud rose **76%** in 2024 (Cifas)

4

Misuse of facility/money mules

What is it?

Criminals recruit individuals, often young people, to move stolen funds through their personal accounts.

How does it work?

Mules are often recruited through social media job adverts that offer 'easy cash' for moving money. Funds are then quickly laundered across multiple accounts.

Why does it spike at Christmas?

Many people experience more financial stress or vulnerability over the festive period, making them prime targets for fraudsters looking to exploit them.

Misuse of facility is the second highest case type recorded to the National Fraud Database in the first half of 2025, accounting for **24%** of all cases filed (Fraudscape)

The eight frauds of Christmas

5

Investment fraud including crypto

What is it?

Fraudsters lure victims into fake investment schemes, cryptocurrency platforms, or wallets with the promise of high or guaranteed returns.

How does it work?

Using slick websites, social media adverts or even cloned celebrity endorsements and fabricated media stories, scammers encourage victims to transfer money or crypto.

Why does it spike at Christmas?

Financial pressure, festive bonuses and year-end 'investment offers' make individuals more receptive to fast-return schemes.

6

SIM Swap

What is it?

Fraudsters trick mobile providers into transferring a victim's phone number to a new SIM card, giving them control of texts, calls and one-time passcodes. Data from Experian shows that that this kind of fraud is up 1,000% from the previous year – with nearly 3,000 cases logged on the National Fraud Database in 2024.

How does it work?

Criminals use stolen personal details and social engineering to persuade providers to activate a fraudulent SIM.

Why does it spike at Christmas?

As businesses and consumers rely heavily on mobile-based authentication during online shopping, SIM swaps can allow fraudsters to bypass Two-Factor Authentication (2FA) and drain accounts.

The eight frauds of Christmas

7

Social media exploits

What is it?

Scams run through fake profiles, bogus adverts, counterfeit marketplaces or phishing messages delivered via social platforms.

How does it work?

Criminals impersonate brands, post fake competitions or run adverts for products that don't exist to harvest money and personal data.

Why does it spike at Christmas?

Seasonal shopping, holiday events and giveaways give scammers easy lures. Customers are also more likely to trust branded promotions as they hunt for the perfect gift.

Action Fraud reported **£224m** stolen during the 2023 festive period

8

Employee-targeted scams

What is it?

Fraudsters impersonate HR, finance or delivery companies to trick staff into handing over credentials, payroll details or make fraudulent payments.

How does it work?

Common ploys include fake eCards with malicious links, spoofed emails offering seasonal bonuses or calls from individuals pretending to need personal information to update payroll records.

Why does it spike at Christmas?

Staff are often distracted, more trusting or covering extra workload. The festive atmosphere also makes scams like 'bonus' offers more believable.

Retail fraud during the holidays

For some retailers, dealing with fraud attempts is a daily activity. But during the holidays, the frequency of these attempts can skyrocket. Here are some of the main tactics fraudsters use:

- Refund and return abuse (from wardrobing, bricking and de-shopping to 'item not received' claims)
- Friendly fraud and chargebacks after legitimate deliveries
- Promo/code abuse using stacking, reselling or coupon bots
- Account takeover driving high-value orders and last-minute address changes
- Delivery disputes that are used to force refunds
- Facility takeover fraud using stolen credentials, bots, spoofed retail sites and delivery smishing campaigns to harvest login details and payment data

These losses are enabled by the unique combination of psychological, financial and logistical changes that happen during the Christmas season. Retailers need to make sure they are aware of the circumstances that enable fraudsters to exploit these seasonal dynamics:

- Relaxed policies such as no-receipt returns or longer windows can become loopholes
- Sheer volume of orders can hide patterns like repeat claimants
- Social engineering of support teams via chat, email or phone can push through overrides
- Synthetic or first-time identities could be used for 'buy now – pay later', click-and-collect and reshipment
- Delivery lures (fake tracking links) steal credentials, enabling account takeover and re-routing

For retailers, the lesson is clear: the festive period is not just about higher sales but also higher risk. Strengthening fraud defences with tiered returns policies, AI-driven anomaly detection, proof-of-purchase requirements and tighter controls on high-risk stock keeping units (SKU) help businesses reduce losses without alienating genuine customers. In the fight against holiday-season fraud, the right balance of friction and fairness protects both margins and reputation.

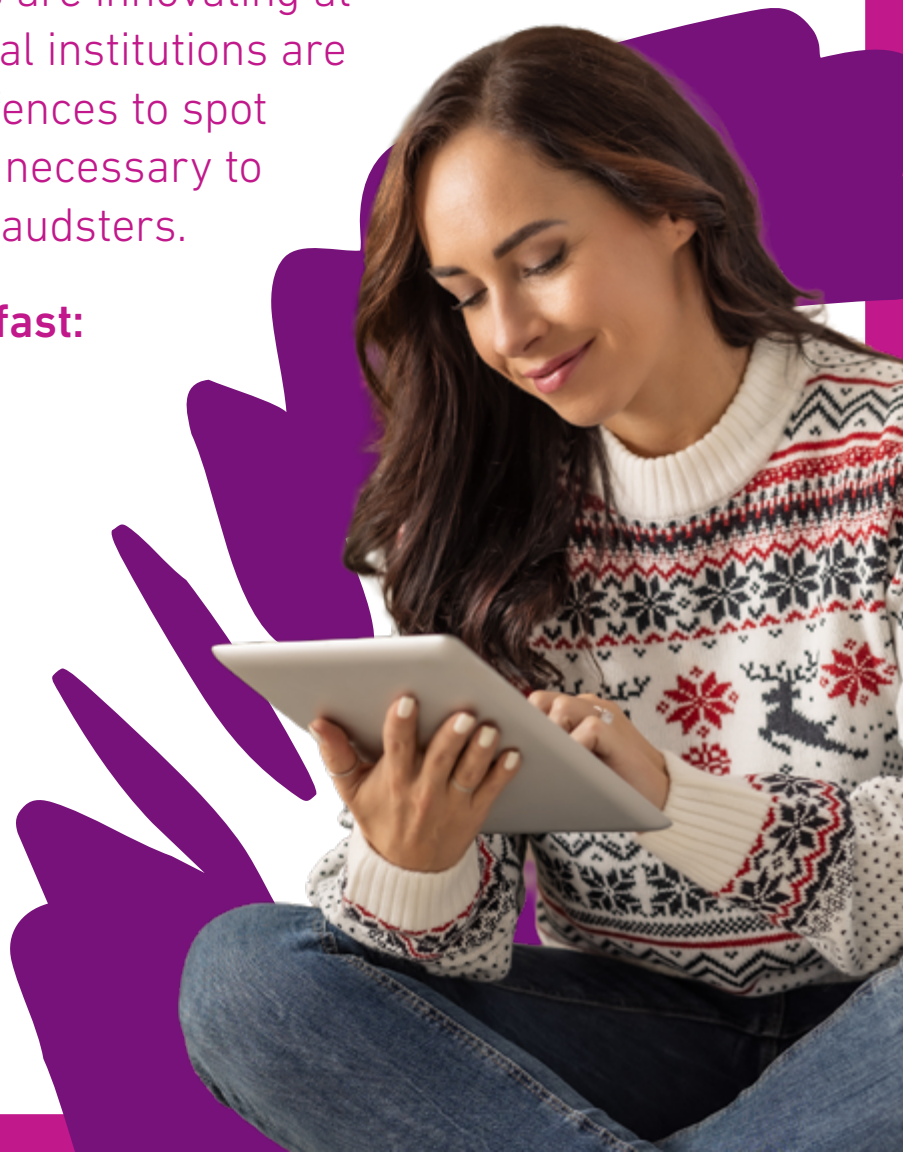
A constantly evolving fraud landscape

The pace of technological change means that the fraud landscape is more dynamic than ever. On both sides, criminals and businesses are innovating at breakneck speed to try and get ahead. Retailers and financial institutions are shifting from static controls to adaptive, intelligence-led defences to spot synthetic IDs and account takeovers in real time. These are necessary to deal with the increasingly sophisticated methods used by fraudsters.

Here are three examples of fraud types that are evolving fast:

Investment scams including crypto target those looking to make money fast

Crypto fraud feeds off the financial pressures that many of us feel over the holidays, especially around events like Black Friday. Cifas and other fraud prevention organisations are concerned that the growing interest in investments scams and 'get rich quick schemes' including cryptocurrency could draw in more victims into fraudulent platforms that offer 'guaranteed returns' that simply do not exist. But these scams don't just harm individual consumers. They also fuel authorised push payment (APP) fraud, expose firms to chargebacks and money-laundering risks, and damage trust when victims link their losses to legitimate brands or payment providers.



Social media scams continue to get more convincing

Social media is now a critical step in the digital buying process for a lot of consumers. It's where people learn about new products, hear announcements from brands or view influencer content. This means that scams taking the form of fake brand pages, bogus marketplace adverts and mule-recruitment job posts can be hard to spot. Research from Experian shows 37% of Brits have experienced a scam on an online marketplace and that losses often reach up to £100 per person. Among those who encountered these kinds of scams, fake or counterfeit products were the most common – making up 34% of the total.

Criminals also monitor genuine brand accounts, intercepting real customer queries to harvest personal details. During the 2023 festive period, Action Fraud reported £224m stolen through online shopping scams, many driven by fake stores and social media promotions. While the huge reach and influence of social media allows criminals to target different demographics on the same platform, it is younger generations that are being targeted most frequently. Almost six in 10 Gen Z consumers surveyed (58%) say they have been exposed to scams compared to 20% of over-55s.

The rise of agentic AI is a gamechanger for fraudsters

Perhaps the most significant shift in recent years is the emergence of agentic AI. These autonomous tools make scams continuous, multi-channel and self-optimising. AI is already being used to craft realistic phishing emails, deepfake communications and persuasive social engineering scripts.

For businesses, this represents a new level of threat. Criminals can automate entire fraud chains from reconnaissance to execution at machine speed to bypass traditional detection. Yet AI is also part of the solution, enabling more effective identity and device intelligence, cross-channel analytics, agent-aware detections and drilled human processes such as 'no change without verify'.

How can you prepare for the holiday season?

Making sure your business is fully protected while still creating a seamless experience for customers is a balancing act. Help reduce the risk by adequately preparing your staff and getting the right processes in place before the rush begins.

Stay sharp through peak season

You don't need to reinvent the wheel. Keep doing what already works and don't let attention to detail slip when teams are lean. Instead, treat November to January as high-alert months. This means pre-approving staff holidays, making escalation routes obvious and empowering people to pause when something feels off.

Make sure your processes are rock solid

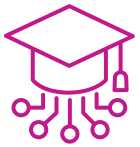
Document the critical steps for payments, onboarding and refunds, and always verify requests through a trusted channel. Make 'no change without verify' a standing rule for supplier details, payroll and access rights.

Increase your visibility

Increase real-time monitoring for account takeover spikes, false applications and payment fraud. Track early-warning signals such as refund velocity, narrative reuse, first-time payment surges and step-up failure rates.

Strengthen customer and user verification

Adopt multi-layered checks (document, device, biometric and behavioural) on logins, account changes, high-risk orders and first-time payments. Many modern solutions will level up verification automatically when risk signals rise, such as a new device, address change or unusual basket.



Increase your training

Run ethical phishing exercises and refresher training on social engineering and internal controls for staff. Explain the reasons behind controls so they feel protective, not punitive. Promoting a speak-up culture also encourages staff to report suspicious emails, odd calls or mistaken clicks immediately.

Get serious about email and identity security

Turn on multi-factor authentication (MFA) for everyone and apply conditional access to risky sign-ins. Monitor for rogue mailbox rules and auto-forwarding, and implement Domain-based Message Authentication, Reporting and Conformance (DMARC), Sender Policy Framework (SPF) and DomainKeys Identified Mail (DKIM) with quarantine/reject so spoofed mail never reaches staff.

Introduce retailer-specific controls

Retailers can apply risk-based SCA and device checks at checkout to keep things moving while staying vigilant. Other options are to tighten refund windows, require evidence for 'item not received', add ID checks for high-risk SKUs and returns, click-and-collect with ID at pickup and locked edits after dispatch, and govern promo codes with rate limits and abuse monitoring.

Build in more steps for payments

Use maker-checker for supplier and bulk payments and confirm any bank-detail changes via a known phone number (never by replying to an email). Add a short cool-off delay before releasing first-time payments.

Protecting your customers

While businesses can't control the choices consumers make around spending their money or sharing personal information, there are steps you can take to support them.

Prioritise account security

Offer and actively encourage MFA on all customer accounts. Back it up with strong-password requirements, automatic logout when behaviour looks risky and instant alerts whenever a customer's email, phone number or address changes. These small nudges close off easy attack paths without adding too much additional friction.

Put the 'check' in checkout

Add confirmation prompts when a new delivery address is entered or an existing one is edited, and apply hold/step-up checks to first-time, high-value orders. This targets risk at the moments fraudsters exploit most but keeps real customers moving.

Support vulnerable customers

Make help easy to find and simple to use. Offer clear guidance in plain language and alternative contact routes beyond email. For higher-risk transactions, offer short cooling-off periods so customers can pause, review and proceed with confidence.

Only collect the data you need

Be transparent about how you use customer information to keep them safe. Clarity builds trust and reduces complaints when additional verification is required.

Customer education

Keep customers one step ahead with timely reminders to shop on trusted sites and marketplaces. Encourage card payments rather than bank transfers to unknown sellers and highlight common delivery scams so they know what to ignore and where to report concerns.

Experian and Cifas' advice to consumers over Christmas

If you've been a victim, then Experian can help clear up your credit report and remove fraudulent information. This can save a lot of time and distress, as we will be able to dispute the information with all relevant companies on your behalf.

- Don't share too much personal information on social media, such as mother's maiden name, home address or when you're away. It's important make sure your privacy settings are up to date across all platforms.
- When you move address, always re-register on the electoral roll as soon as you can. This helps ensure your details are no longer registered at your previous address. It's a good idea to set up mail redirection for a while too.
- Make sure you have an individual unique password for each online account you have. This means fraudsters are less likely to gain access to multiple accounts.
- Ensure your home Wi-Fi has a strong password, never sign in in to password protected accounts on unsecured public Wi-Fi and make sure you have up-to-date antivirus software
- If you receive emails or text messages always be cautious about attachments, links or telephone numbers. If in doubt, visit the company website and contact them directly.
- Keep your private documents safe at home, and be careful traveling with important ID documents. Always destroy mail or documents with personal information if it's no longer needed.
- Check your credit report, for free, on at least an annual basis to look for anything suspicious. This will show any applications for credit or new accounts. You can also monitor your free Experian Credit Score to look for any significant changes.

Experian and Cifas' advice to consumers over Christmas

If you find you've been a victim of identity fraud, there's also lots of support available:

- Check your free statutory credit report, with all three credit reference agencies. You can then review all information that does not belong to you.
- Contact any relevant lenders to inform them of the fraudulent information
- Ask Experian, or a credit reference agency, to dispute the fraudulent information with all relevant companies and lenders. A notice of dispute will also be added to the fraudulent information.
- Add a password to your credit report. this is called a Password Notice of Correction, and should be unique and only known to you.
- Add self-registration details with Cifas, the UK's fraud prevention service. A credit reference agency can sometimes do this for you.
- Contact Action Fraud, the UK's national reporting centre for fraud and cyber crime.

Working together to make sure this holiday season is the most wonderful time of the year

The festive season is a time for celebration, but for businesses it carries heightened risk. Fraud consistently spikes between November and January in line with increased online spending and stretched operations. Threats like identity theft, account takeovers, social media scams and AI-powered deepfakes are varied and fast-moving.

While you can't switch off fraud, you can stay one step ahead of it. By treating the end of the year as high-alert months, businesses can keep both their customers and their operations protected. With the right planning, layered defences and a culture of vigilance, everyone can enjoy the holidays knowing their organisation is as resilient as possible.

Experian is a market leader in fraud prevention technology and has prevented more than £10.7bn in fraudulent applications over the last five years.

Cifas is the UK's fraud prevention service, a not-for-profit membership organisation that helps businesses, public sector bodies and law enforcement prevent and detect fraud and financial crime.

Registered office address:
The Sir John Peace Building, Experian Way,
NG2 Business Park, Nottingham, NG80 1ZZ

www.experian.co.uk/business