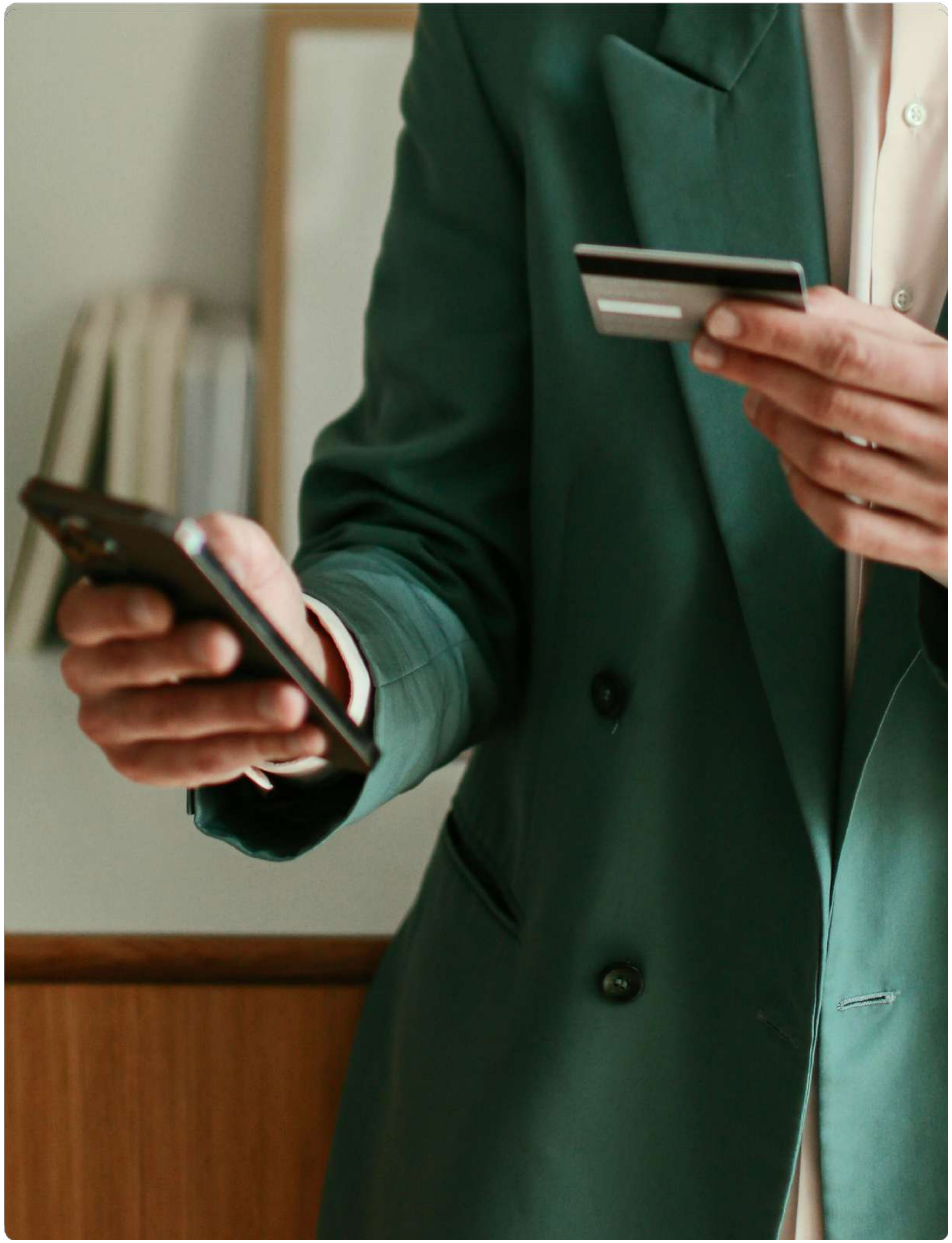
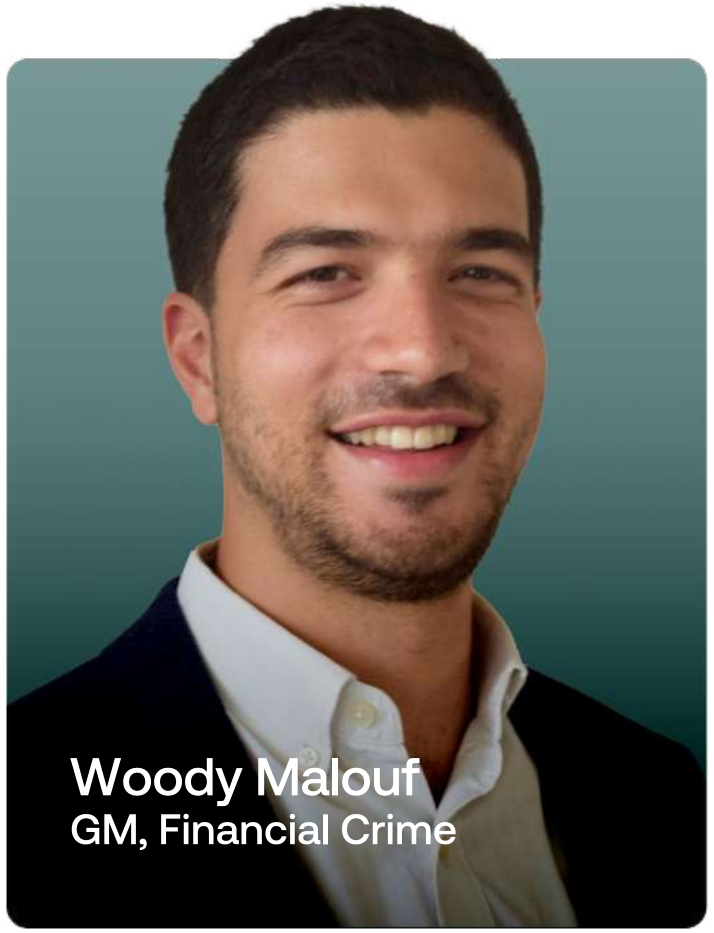
Revolut

Consumer Security and Financial Crime Report FY25



Revolut Group Holdings Ltd
Registered number: 12743269



Woody Malouf, General Manager, Financial Crime at Revolut, on the fourth edition of our Consumer Security and Financial Crime Report

The landscape of global fraud is evolving at pace. As we release the fourth edition of Revolut's Consumer Security and Financial Crime Report, we find ourselves at a critical juncture. While our defences have never been stronger, the adversaries we face are increasingly sophisticated, leveraging new technologies and platforms to attempt to exploit consumers at scale.

At Revolut, we have always believed that technology is our greatest weapon. Our proprietary fraud detection system processes billions of data points in real-time. However, as this report reveals, the "front line" of fraud has moved far beyond the borders of financial platforms.

Insights from 2025

In 2025, our teams analysed billions of transactions. This massive dataset allows us to look past the noise and identify the true engines of the fraud economy. The findings in this year's report underscore several pivotal shifts:

- **Meta remains dominant, but Telegram is on the rise:** While Meta-owned platforms remain the largest single source of Authorised Push Payment (APP) fraud, we are witnessing a dramatic surge in activity on Telegram. It has rapidly expanded to rival traditional social networks as a primary channel for criminals.

- **Scammers are shifting:** Fraudsters are pivoting their tactics. Job scams have emerged as the fastest-growing category, more than doubling year-on-year, preying on economic vulnerabilities. Conversely, while purchase scams remain the most frequent, we are seeing a welcome decline in impersonation scams in key markets like the UK - a testament to improved consumer awareness and bank-level interventions.

- **The need for cross-sector accountability:** The data is clear: financial institutions cannot solve this in a vacuum. A significant majority of scams originate on social media and telecommunications networks. To truly protect the global financial ecosystem, we must move toward a model of mandatory accountability for the platforms where these scams originate.

What this report covers

This edition serves as both a strategic analysis for the industry and a practical guide for our users. Inside, you will find:

- **A deep dive into the most prevalent fraud types and their shifting growth rates.**
- **An analysis of the primary sources of fraud, highlighting the role of non-financial platforms.**
- **An overview of the innovations Revolut has deployed this year to neutralise threats.**
- **Actionable safety protocols to help our customers outsmart even the most "ruthless" criminal tactics.**

Our priority remains steadfast: keeping customers safe. We will continue to innovate, advocate for systemic change, and provide the transparency needed to turn the tide against financial crime.

Contents

4 Methodology + what is fraud?

5 Types of unauthorised fraud

6 Types of authorised fraud

7 2025 Global fraud + scam trends

8 Prevalence and impact of authorised vs. unauthorised fraud

Exhibit 1 - Authorised Fraud vs. Unauthorised Fraud: distribution of victims (FY24 - FY25)

9 Authorised fraud deep dive: global overview

10 Where does Authorised Fraud most commonly originate?

Exhibit 2 - Authorised fraud by source of origination FY25 (% of total victims of Authorised Fraud)

11 Which APP scams are most prevalent?

Exhibit 3 - Top 3 types of APP scams in FY25

Exhibit 4 - Authorised Fraud APP breakdown by type of scam - (FY24 vs FY25)

Exhibit 5 - Average amount loss per victim (FY24 vs FY25)

Exhibit 6 - Comparative losses across scam types (FY25)

13 Fraud origination by platform

Exhibit 7 - APP scam origination by social media platform (FY25)

14 Fraud origination by country

Exhibit 8 - APP scam origin platform by country (FY25)

Exhibit 9 - APP scam type by country (FY25)

14 Fraud origination by age group

Exhibit 10 - Distribution of APP scams by age group (FY25)

16 How to identify a scam

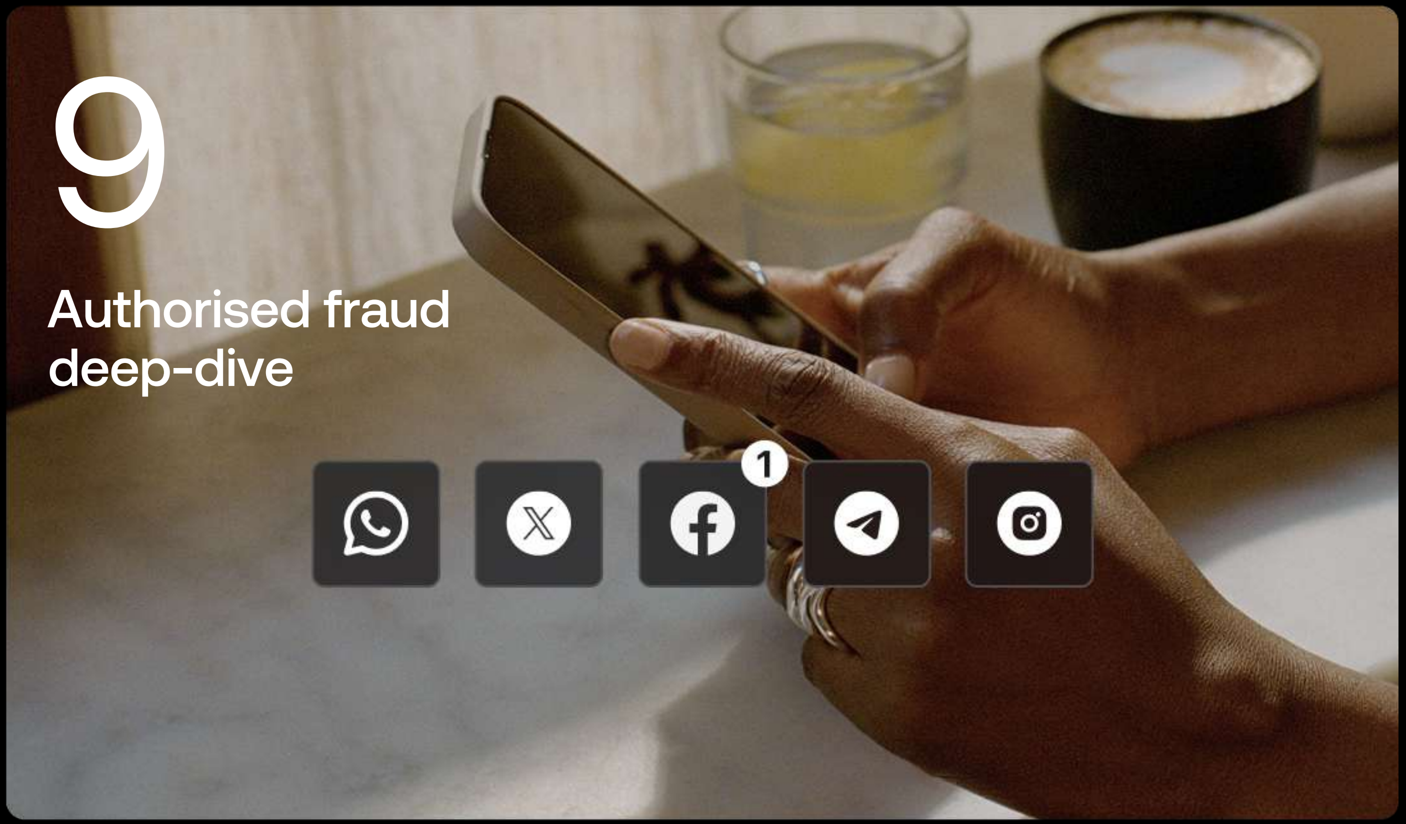
18 Unauthorised fraud deep dive: global overview

19 Exhibit 11 - Unauthorised Fraud breakdown by type of fraud (FY25)

20 How Revolut is fighting fraud

21 Revolut's security features

23 Conclusions



9

Authorised fraud deep-dive

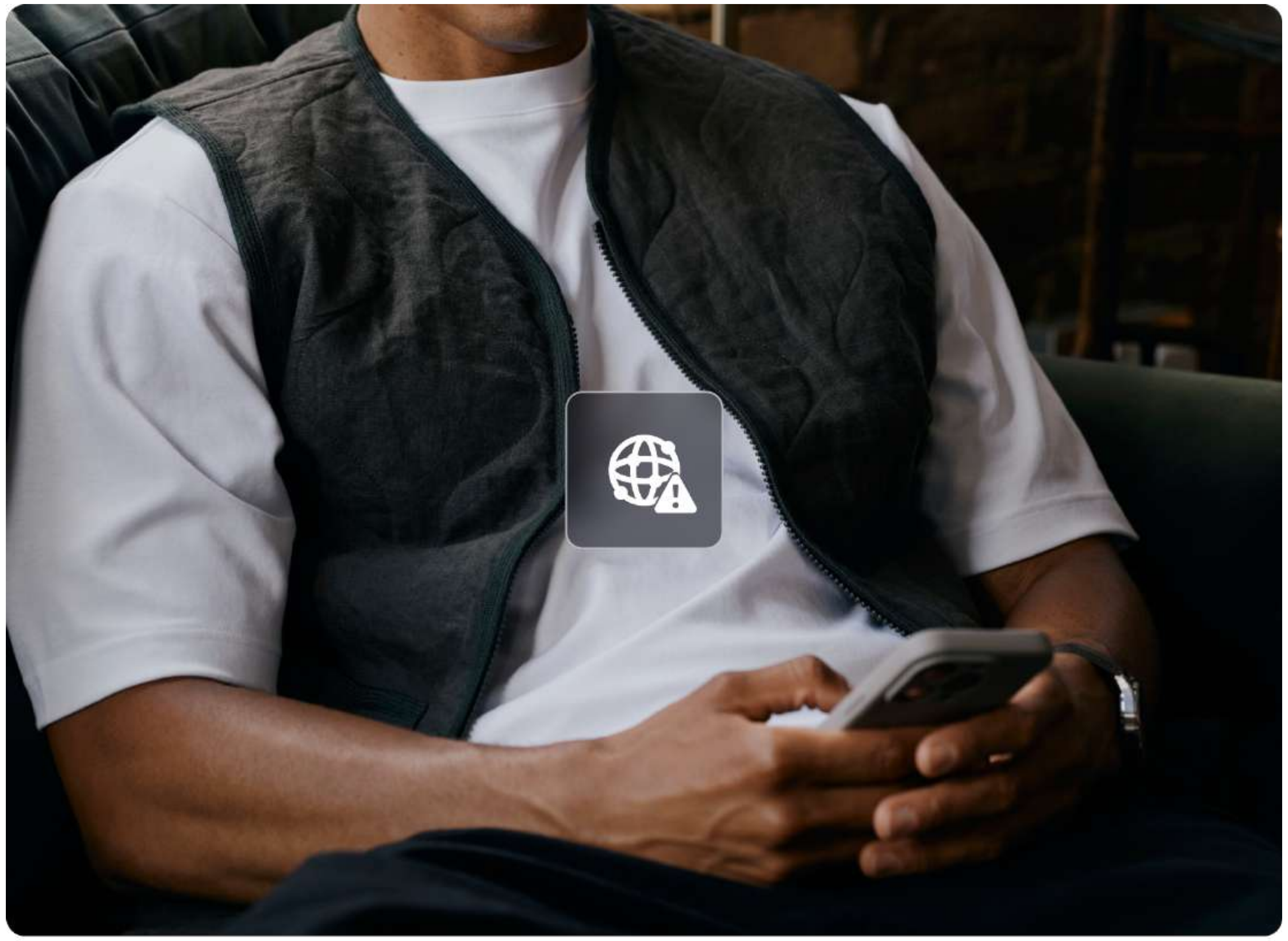
20

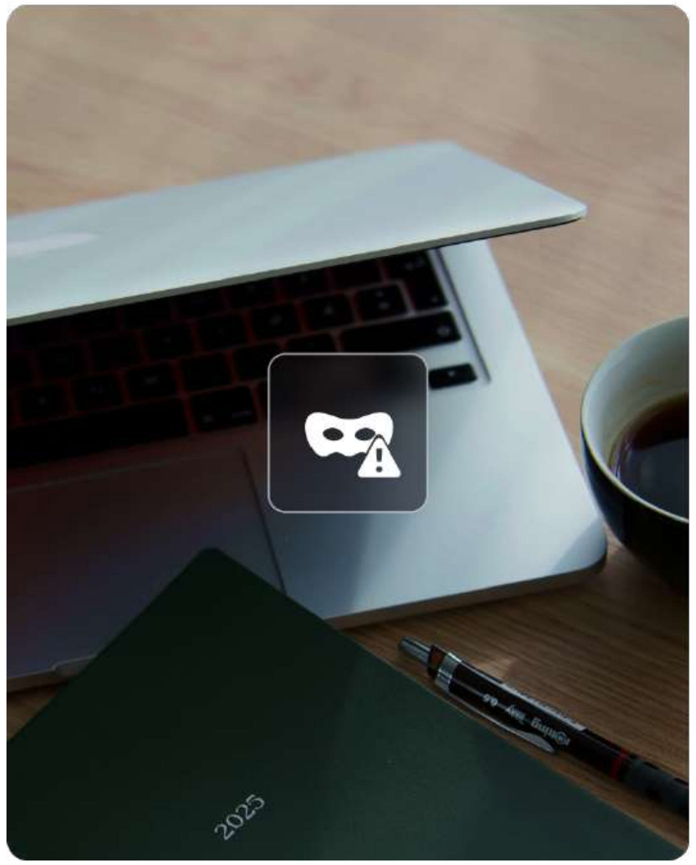
How Revolut is fighting fraud

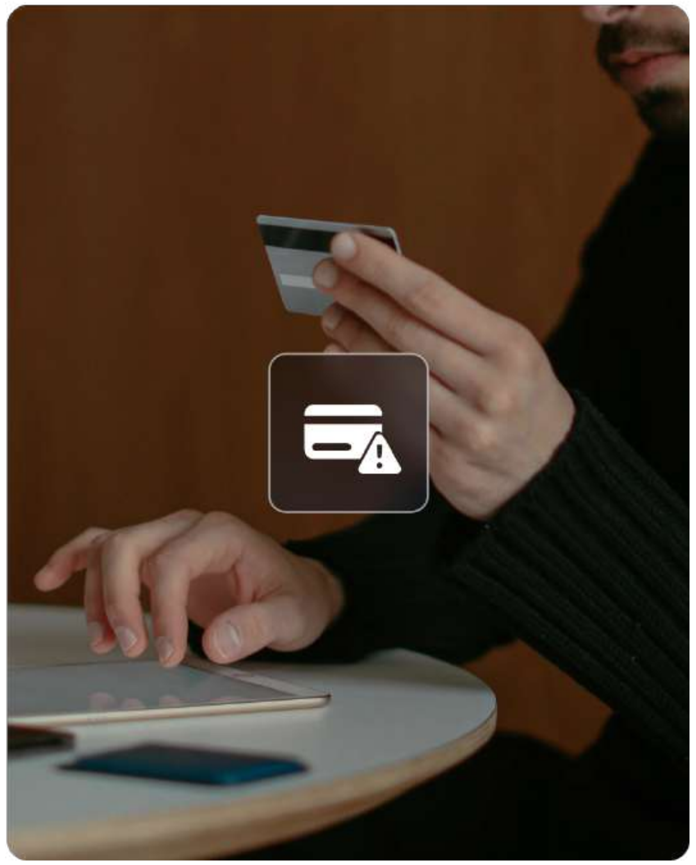
23

Conclusions

Methodology + What is fraud?







Methodology

The findings in this report are based on anonymised data from the Revolut platform, spanning a 12-month period between 1 January 2025 - 31 December 2025. The data covers all fraud reported to Revolut — however, we acknowledge a proportion of fraud goes unreported

What is Fraud?

Fraud can be categorised into two main types: unauthorised fraud and authorised fraud.

- **Unauthorised fraud** occurs when individuals unlawfully access another person's money, sensitive information, or assets. This form of fraud involves gaining unauthorised access to personal details, which may then be used to take over accounts, initiate unauthorised payments, or apply for credit cards in the victim's name.

- **Authorised fraud**, or a 'scam', involves deceptive tactics where fraudsters trick individuals into making payments or transferring money. These scams often present as enticing offers or trusted entities and use various methods, such as fake phone calls, texts, emails, or social media posts, to persuade victims to part with their money.

Types of unauthorised fraud

There are many types of unauthorised fraud. The three key ones Revolut customers are exposed to are:

- **Remote Account Takeover:** Fraudsters gain access to a customer's account by obtaining security credentials or account information through digital or non-digital means - such as phishing, malware, or social engineering - and then use a different device to make payments or transfer funds.

- **Physical Account Takeover**: This occurs when a fraudster steals the customer's device and compromises its security, allowing them to access the account on the existing device and carry out unauthorised transactions.

- **Unauthorised card fraud:** this is when a fraudster gets access to a customer's card details, and then uses it to make transactions that the customer is not aware of.

Types of authorised fraud

Authorised fraud can be divided into different categories based on the payment method, such as authorised push payment fraud (APP) or authorised card fraud.

This distinction is important for the industry, as payment methods may be exploited differently and can have different levels of traceability, reducing the likelihood of victims recovering their funds.

Authorised fraud is further classified by the tactics used to deceive customers:

Impersonation scams

Impersonation scams occur when fraudsters pretend to be trusted entities

Scammers may pretend to be bank, government or commercial agents contacting you about unsafe accounts, unusual activity, or unpaid fees, taxes or loans. They might sound serious, asking for immediate payments or personal details to fix supposed issues.

Purchase scams

Purchase scams are when victims are convinced to pay for goods or services that do not exist, are never delivered, or are not as advertised

Fraudsters may trick victims with fake websites or marketplace adverts that promise products which are never delivered. Rental scams are also considered a type of purchase scam, where fraudsters list fake rentals and ask for upfront deposits from potential renters.

Romance scams

Romance scams involve fraudsters utilising fake online profiles to form a romantic relationship with a victim

Scammers create a new romantic connection with the victim, building up trust over weeks or months. Fraudsters may then ask for some money using an emergency or travel plans as an excuse, before disappearing.

Subscription scams

Also known as mandate fraud, this is when fraudsters pose as a subscription service, merchant, or service provider.

Fraudsters may use fake invoices to trick victims into making payments. This type of fraud often only comes to light when the genuine merchant or service seeks payment.

Loan scams

A loan scam is a form of fraud where scammers pretend to be legitimate lenders offering loans

Fraudsters might offer cheap loans to their victims, with minimal collateral and application fees needed. However, once the victim has paid the application fee or deposit, the victim never receives the loan.

Investment scams

An investment scam is when someone tricks victims into giving them money for fake investments

Fraudsters may convince users to transfer funds or cryptocurrencies by offering fake investment opportunities with lucrative returns. A common investment scam tactic involves using investment news articles or fake social media posts — seemingly endorsed by celebrities — to highlight opportunities for consumers to make high returns on their money.

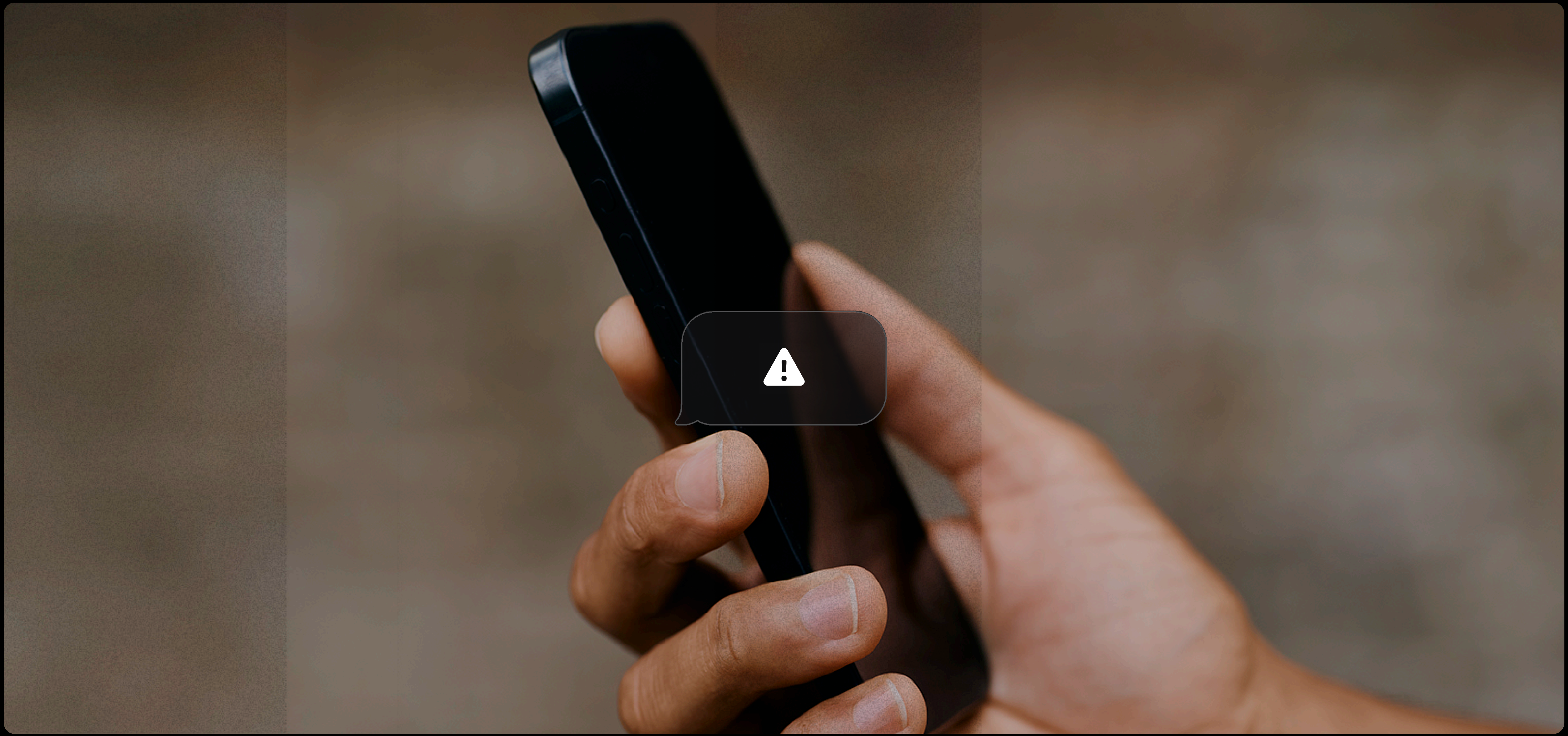
Job scams

A job scam is a fraudulent offer of employment designed to steal money or personal information from job seekers

Scammers may post fake online job openings, or reach out via messaging apps for job openings. As part of the application, they either request money upfront, or require personal financial information to defraud the victim. This could look like asking people to pay upfront for training or administration fees, or purchase equipment, such as a laptop or phone.

Alternatively, scammers could offer small commissions for completing tasks, then encourage victims to deposit higher-value funds to benefit from time-limited increases in commission.

Global fraud and scam trends



Prevalence and impact of authorised vs. unauthorised fraud

All the data, charts, and tables refer to Revolut Retail fraud reported in the calendar year 2025, unless specified otherwise.

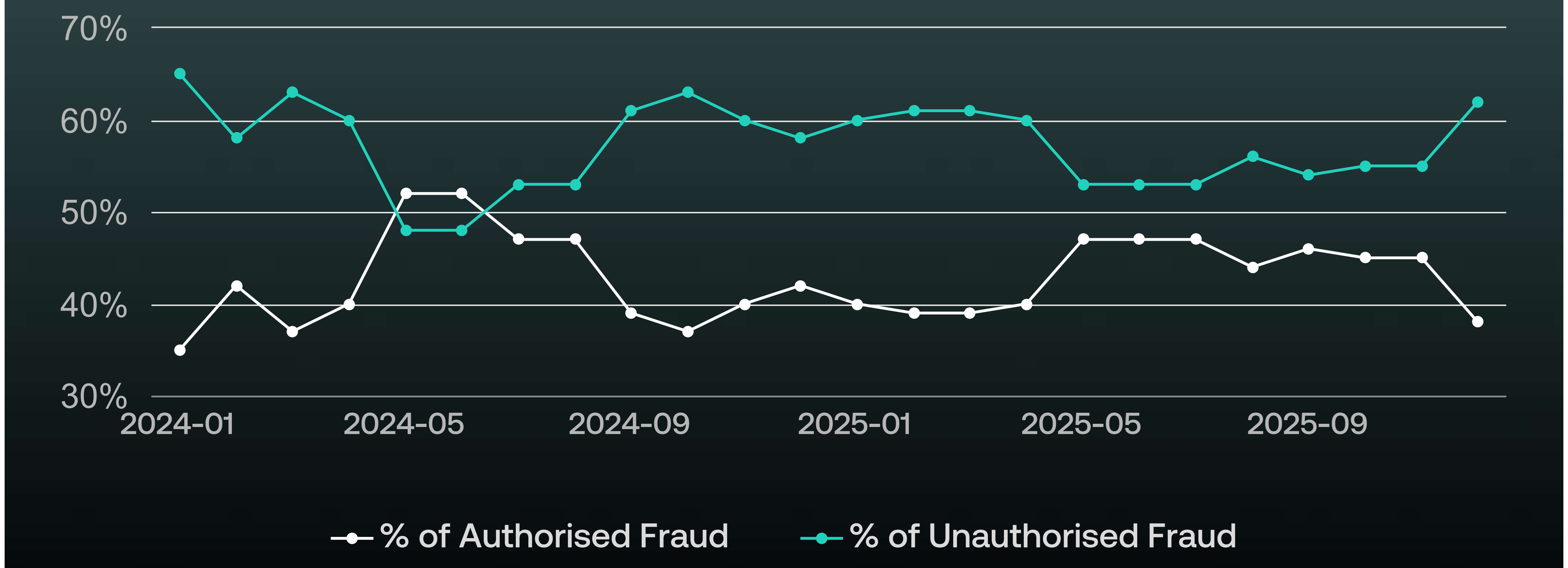
Distributions of authorised and unauthorised fraud remain unchanged in 2025 compared to 2024. On average, unauthorised fraud accounts for 60% of all cases, and authorised fraud around 40%. (Fig. 1.)

Although unauthorised fraud is still more prevalent, the latest data shows that the average loss from authorised fraud is 13 times greater than that of unauthorised fraud, up from 12x reported in 2024.

Social engineering tactics are becoming more and more convincing with the proliferation of AI, as fraudsters develop more persuasive ways to exploit individuals' trust. Financial institutions like Revolut are at the forefront of this battle, investing in advanced technology and education to protect consumers. However, as we will see from further analysis, new cross-platform initiatives such as additional safeguards and data sharing are key missing pieces in the fight against evolving forms of fraud.

● Authorised Fraud vs. Unauthorised Fraud: share of victims

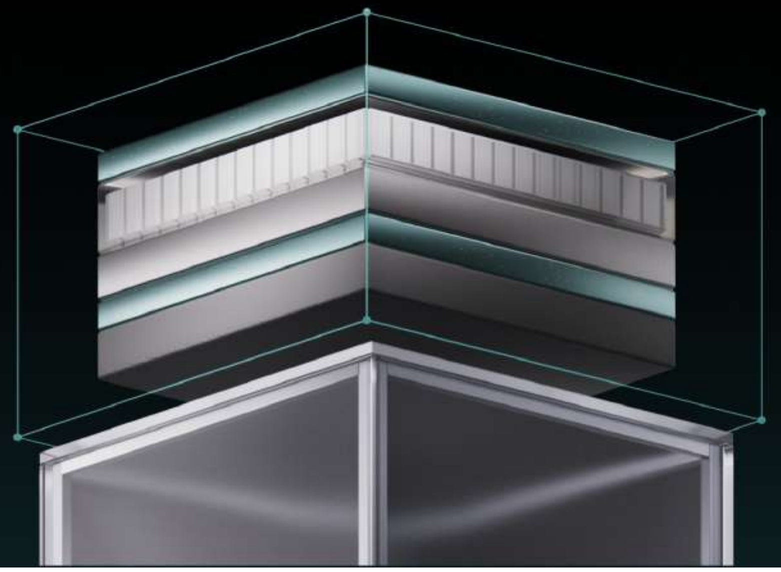
Exhibit 1



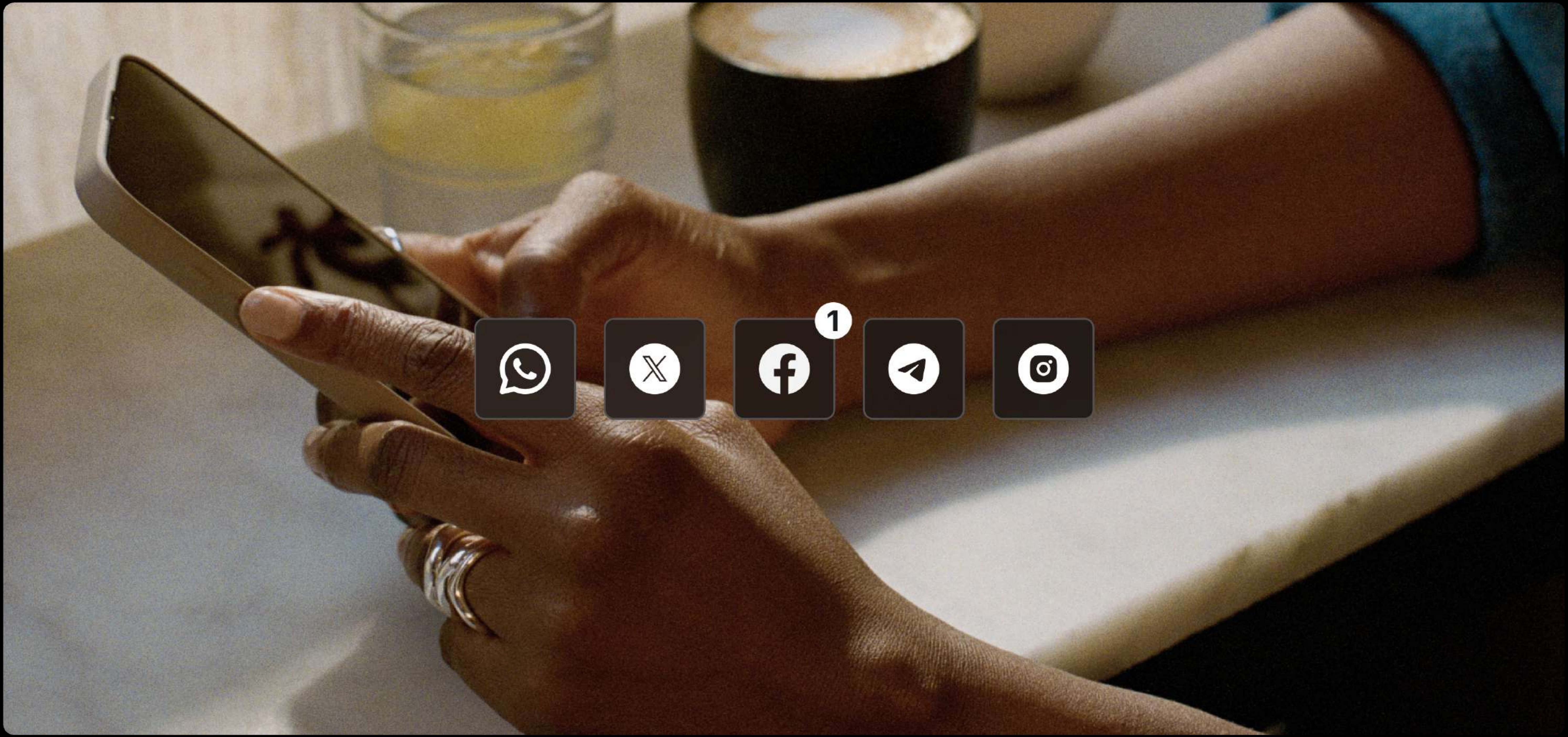
● Authorised Fraud vs. Unauthorised Fraud: Average losses per victim (FY25)

13x

Authorised fraud



Authorised fraud deep-dive: global overview



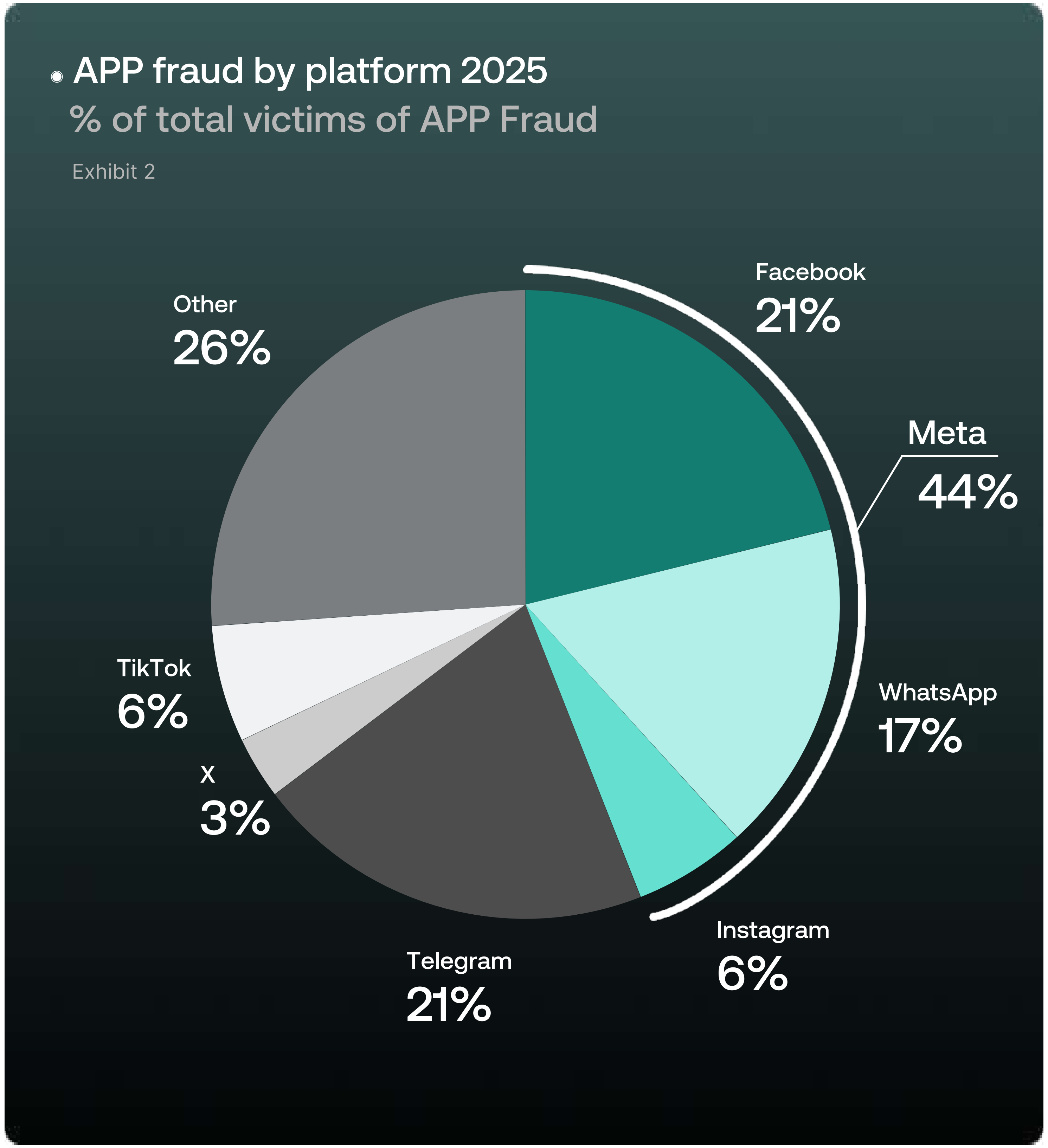
Where does Authorised Fraud most commonly originate?

Meta maintains its lead: For the fourth consecutive reporting period, Meta remains responsible for the largest share of authorised fraud. Although its overall share has dropped to 44% (down from 58% in 2024), this is driven by an increase in scam activity on other platforms, and given the lack of clear reportable metrics we've seen no evidence that the reduction reflects improvements from the initiatives Meta has been rolling out. For the third year in a row, Facebook leads on authorised fraud, accounting for over 21% of all cases in 2025, with WhatsApp accounting for a further 17%.

Telegram now level with Facebook: The proportion of scams coming from Telegram has continued to grow in 2025, following trends shared in the previous report. The platform now accounts for over 20% of authorised fraud origination, overtaking WhatsApp and growing by over 30% in its share of scam cases compared to 2024.

TikTok's rapid increase: Although overall volumes of authorised fraud sourced from TikTok are still relatively low, there has been a 6x increase in the number of users reporting TikTok as the origin of scams. Criminals are capitalising on the success of TikTok's e-commerce marketplace, TikTok Shop, and leveraging increased user activity to boost the reach of their scam ads.

Fraud is a growing threat across all platforms: Social media platforms such as Discord, Reddit, and Snapchat fall into the category of 'Other'. While on an individual basis their shares remain low, the fraud spreading across these platforms accounts for over 1/5 of reported fraud. Marketplaces such as Airbnb, eBay, and Ticketmaster are also included in this group, and the variety within this data set illustrates that fraud is an industry-wide problem, and must be tackled systematically at every level.

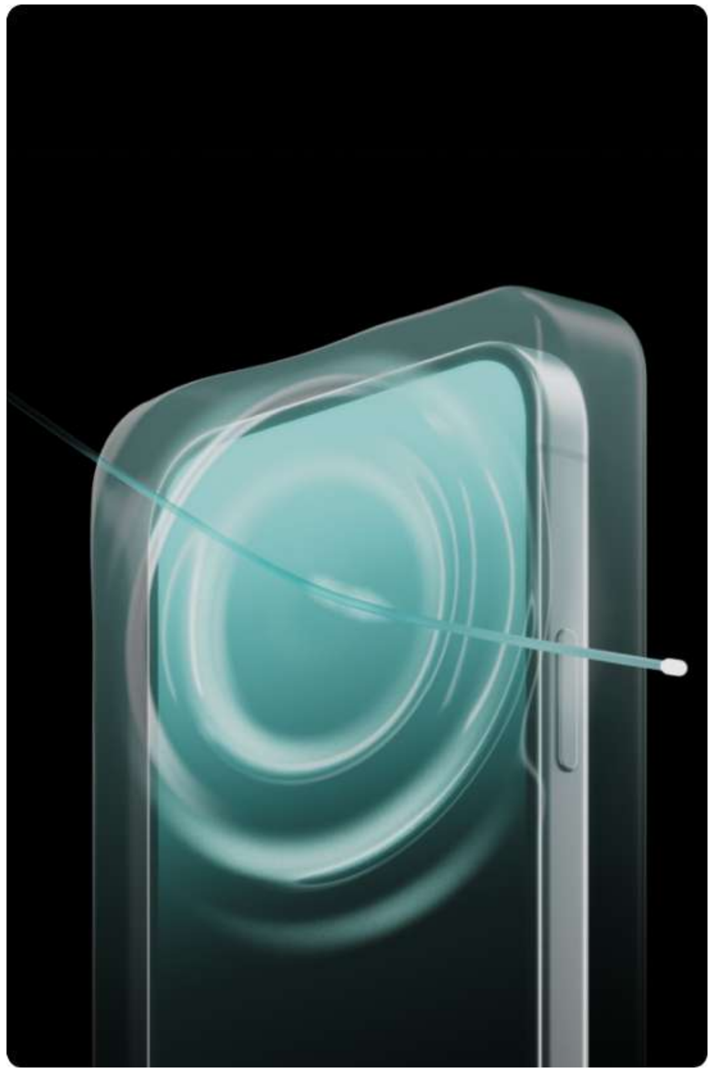

APP fraud by platform 2025

% of total victims of APP Fraud

Exhibit 2

Financial institutions can only implement controls once a scam is already under way; blocking the dissemination of this content at its source is a key missing piece in the fight against fraud. The data continues to show the urgent need for social media platforms to participate in cross-industry initiatives to effectively stop fraud at its source.

To dive deeper into how and where authorised fraud commonly originates, we'll now take a look into the trends in scams, where they arise, and how they operate.



Which authorised scams are most prevalent?

Purchase scams
Purchase scams continue to be the most prevalent type of APP scam, accounting for nearly 57% of all reported scams in 2025. Their ease of execution means they proliferate on resale platforms and social media marketplaces. The share of purchase scams remains unchanged from 2024, highlighting the continued prevalence of scam ads on these platforms. (Fig. 3.)

In fact, a report from Juniper Research found that European users were served nearly 1 trillion scam ads in 2025. The average user now encounters 190 scam ads per month, a figure projected to rise to 250 by 2030 if current trends persist.

Although purchase scams continue to dominate, there are other scam types that significantly impact customers, namely:

- **Job scams:** more than one in five (22%) of APP fraud victims has been targeted by a job scam in 2025, compared to the 18% share held in 2024. This scam type saw the most significant increase year over year, highlighting how scammers continue to take advantage of applicants searching for employment.
- **Investment scams**: almost 10% of all scam victims were impacted by investment scams, although the data shows a slight decrease in comparison to 2024.

Top 3 types of APP Scams

57%

of APP cases were **Purchase Scams in 2025**

22%

of APP cases were **Job Scams in 2025**

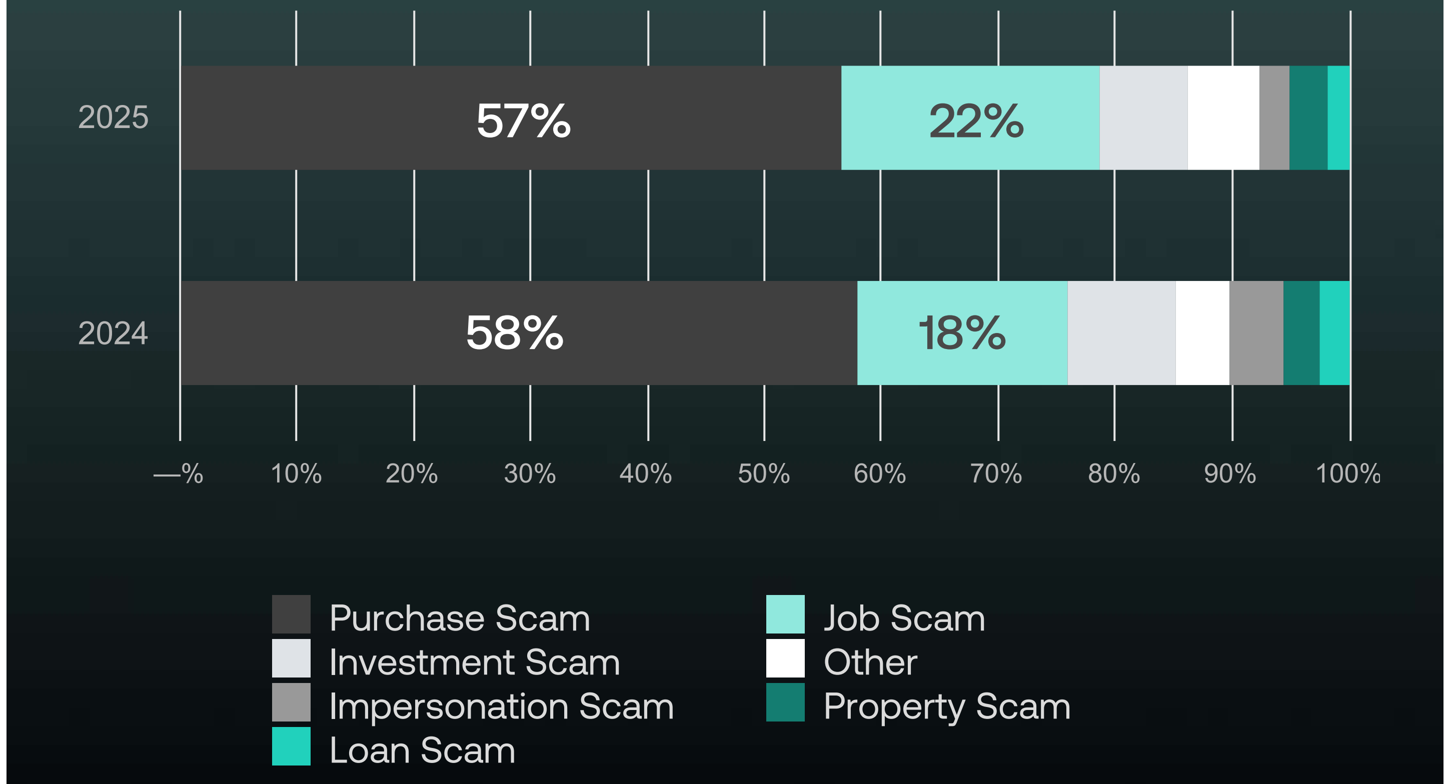
10%

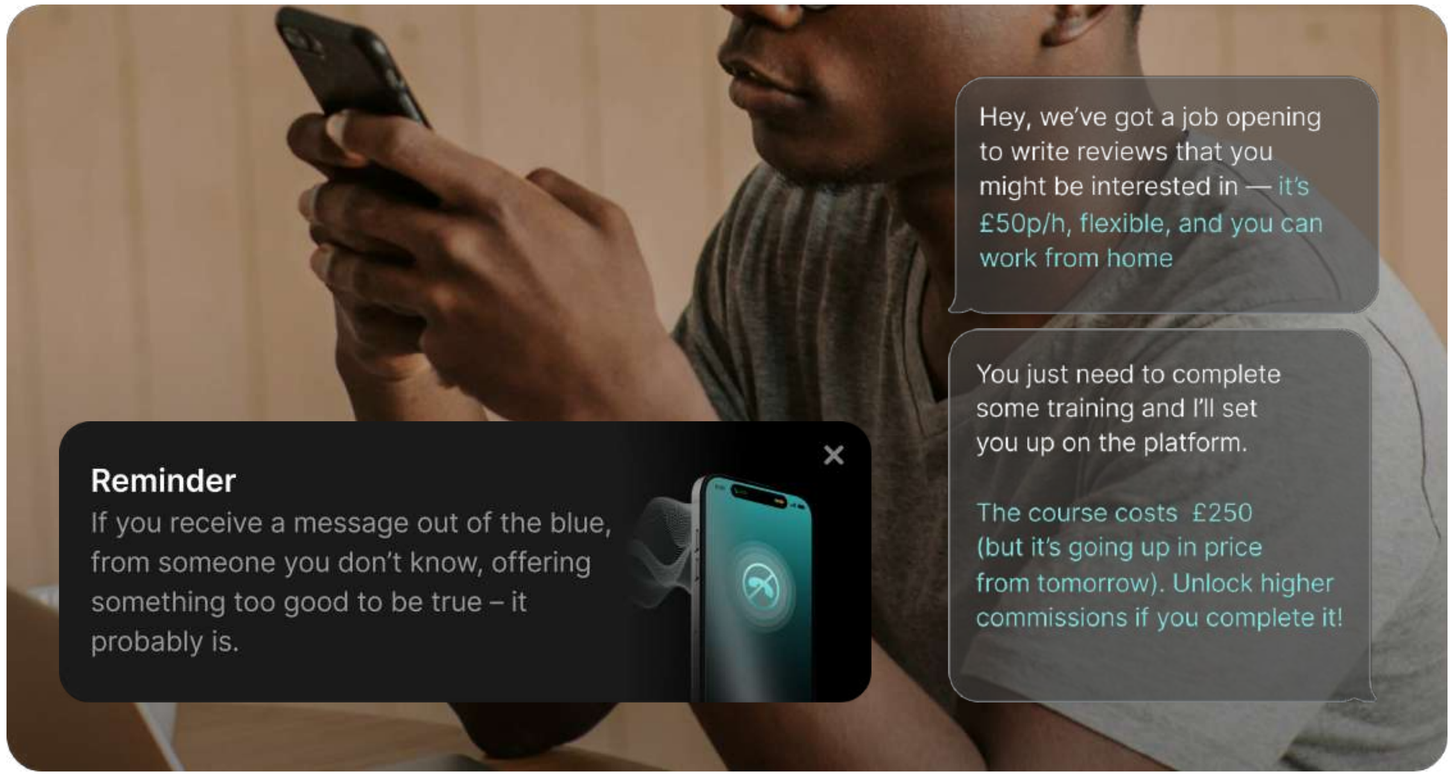
of APP cases were **Investment Scams in 2025**

Exhibit 3

Share of scams by % victims (2025 vs 2024)

Exhibit 4





Hey, we've got a job opening to write reviews that you might be interested in — it's £50p/h, flexible, and you can work from home

You just need to complete some training and I'll set you up on the platform.

The course costs £250 (but it's going up in price from tomorrow). Unlock higher commissions if you complete it!

Reminder
If you receive a message out of the blue, from someone you don't know, offering something too good to be true – it probably is.

The data also reveals notable trends in the average amount lost to each type of authorised fraud.

On average, those targeted by investment and impersonation scammers are likely to lose 12x the amount lost by victims of purchase scams, highlighting the devastating impact of these long-term cons.

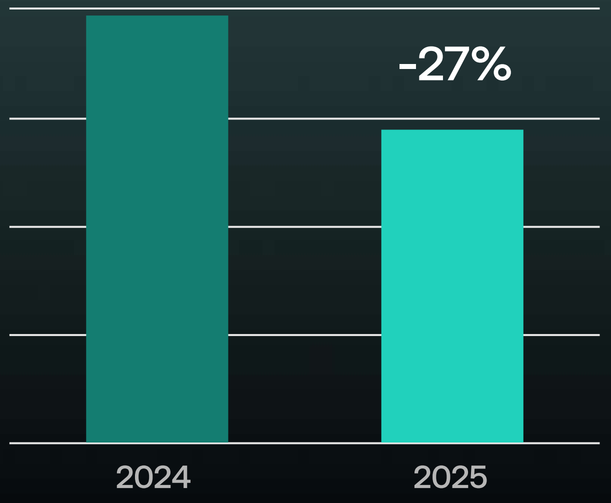
However, compared to 2024, we observe a positive trend; **a 27% reduction in average amount of money lost per scam.**

This data indicates that, due to our controls, customers are losing less to typically higher-value scams such as investment, job, and property scams. However, one crucial outlier to this trend was impersonation scams, which saw a 6% increase in average losses compared to 2024.

Although often lower value, purchase scams continue to proliferate unchecked, emphasising the need for social media platforms to step up and stem the rise of scam ads.

Average amount lost (£) per victim

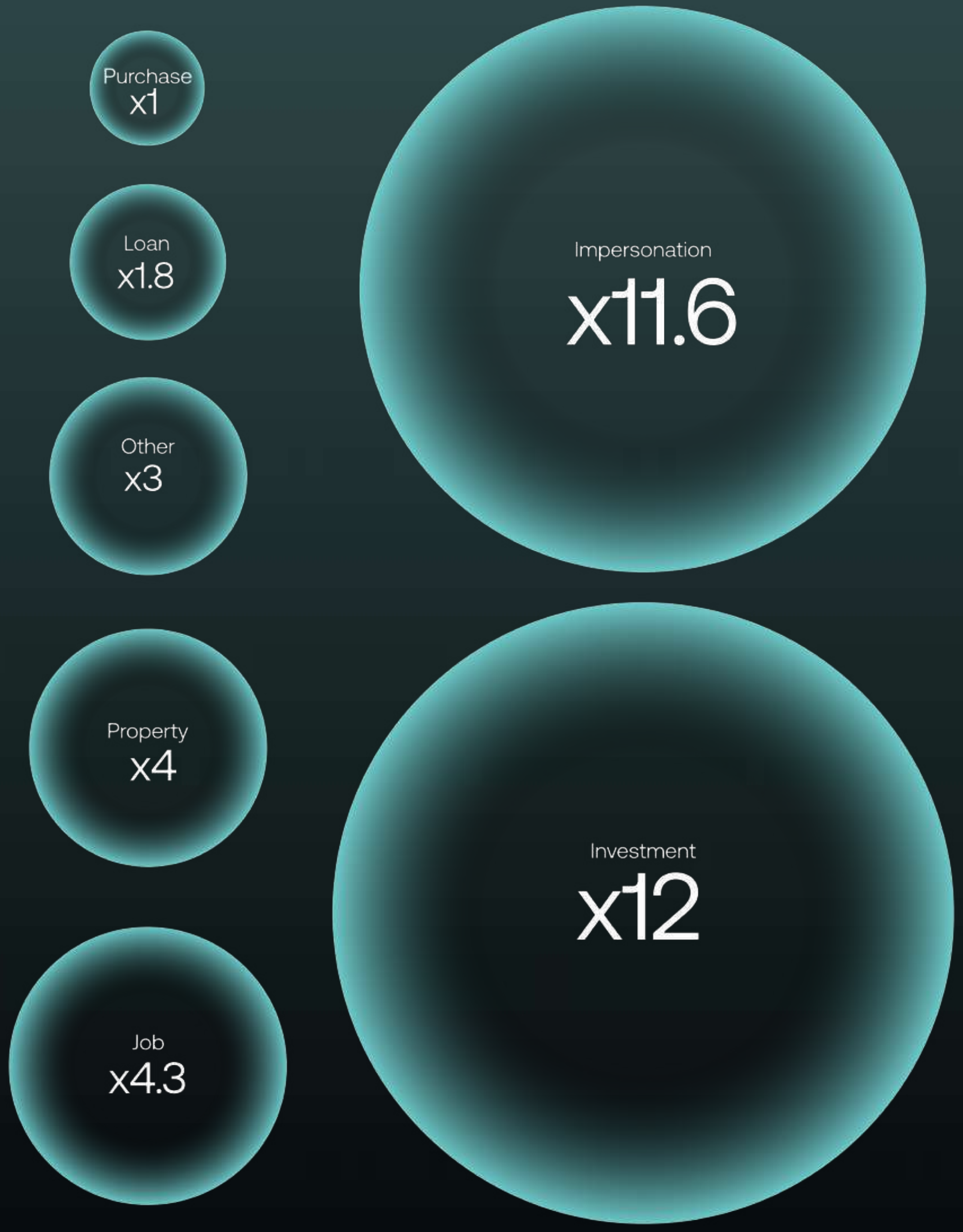
Exhibit 5



Comparative losses across scam types

Victims of investment scams lose up to 12x more on average than victims of purchase scams

Exhibit 6



Fraud origination by platform

Meta-owned platforms continue to be the main source of all APP scams, accounting for 44% of all reported scams.

In particular, purchase scams are rife across Meta, accounting for 55% of this type of fraud. Between them, Facebook, WhatsApp and Instagram also generate over 50% of all loan and property scams. WhatsApp is the worst offender, accounting for over 30% of both loan and property scams, emphasising the prevalence of APP fraud perpetrated via direct messenger.

Combined, direct messaging platforms WhatsApp and Telegram account for 60% of investment scams - as well as an astounding 79% of all job scams.

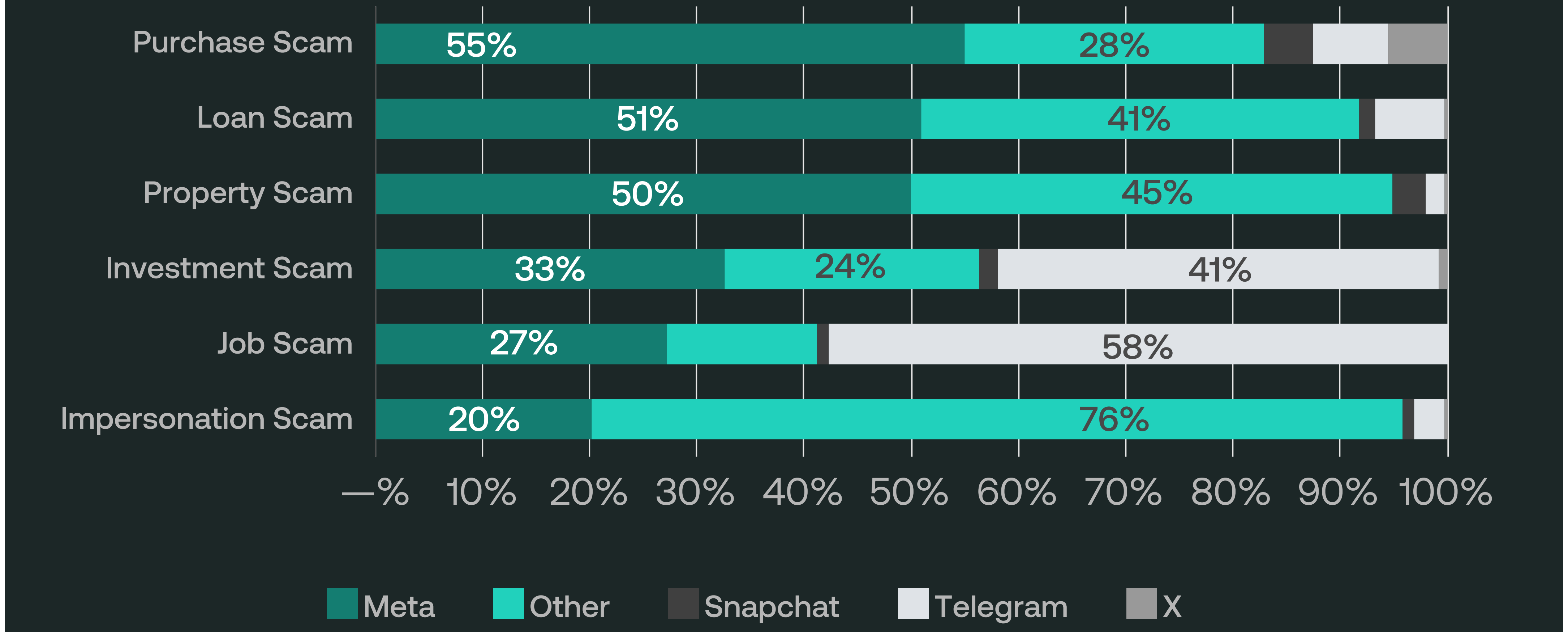
Here, we see another concerning trend - **Telegram alone now accounts for over 58% of all job scams**, up from 50% in 2024. It is clear the messaging platform must urgently step up and implement controls to combat these types of fraud.

The rise in instances of APP fraud originating on 'secure' messaging platforms emphasises the need to develop targeted strategies for each type of APP scam, ensuring the safety of customers in both public and private domains.

● APP scam origination

by % Social Media platform

Exhibit 7



Fraud origination by country

Platform breakdown
In all countries, Meta-owned platforms collectively represent the largest source of authorised scams.

Facebook is the leading single platform for scam origination in 65% of the countries mentioned in this report, with over one in three scams reported in Malta (52%), Norway (49%), Denmark (47%), Hungary (46%), Slovenia (57%), Ireland (38%), Australia (38%), the Czech Republic (35%), and Brazil (34%) attributed to the platform. WhatsApp leads in a further 4 countries, with nearly one in five scams in the UK (22%), and Romania (22%), as well as one in three in Brazil (32%) and one in six in Switzerland (16%) originating on the messaging app.

Alarmingly, Telegram has taken the lead as the single largest scam source in 23% of included countries, particularly in Western Europe. Telegram now accounts for one in three scams in Italy (34%) and Latvia (31%), and one in five scams in Germany (27%), France (25%), Spain (23%), and Belgium (23%), emphasising the proliferation of fraud over direct messenger apps.

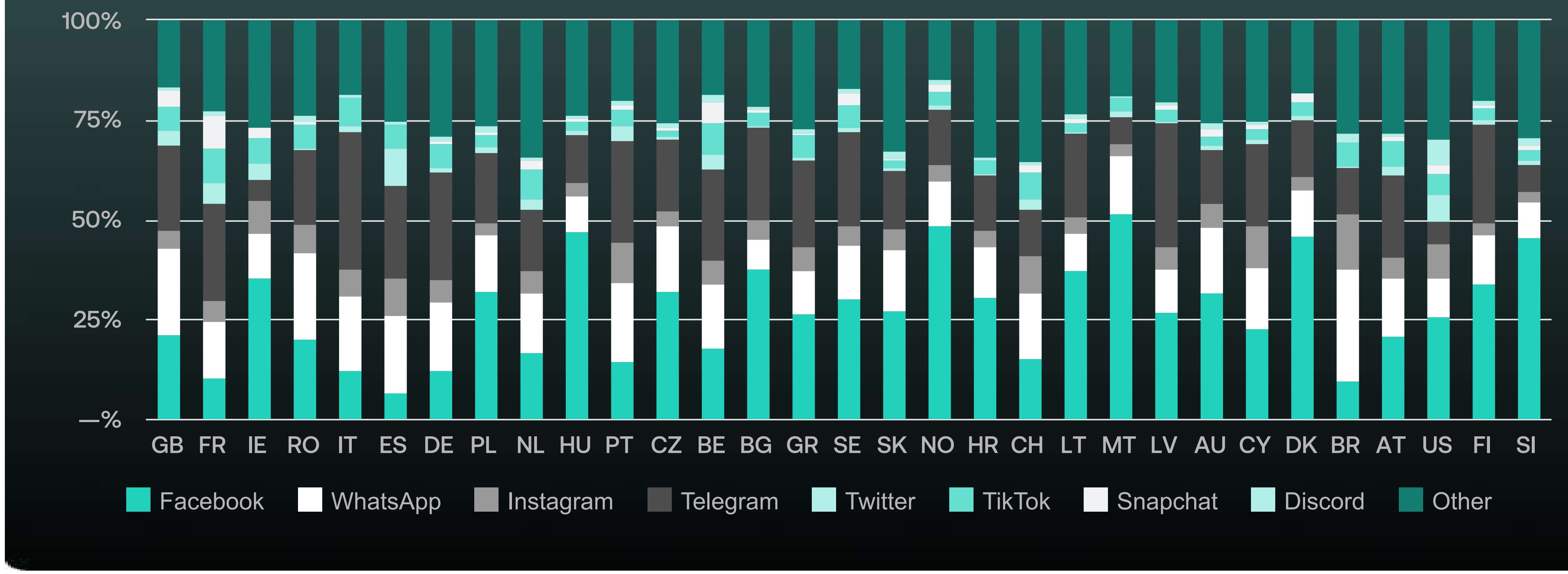
Purchase scams prevail
Due to the ease of dissemination, purchase scams are the dominant scam type in all included markets. Ireland continues to be a stand-out (76%), as well as Slovenia (78%), Norway (72%), and Hungary (71%). Purchase scams are also overwhelmingly dominant in the US, making up 78% of all scams reported.

Job scam spikes
After purchase scams, job scams take up the second largest share of reported fraud. This is particularly prevalent in Western Europe, which reported 80% of all job scams in 2025. Countries most significantly affected include Italy (34%), France (30%), Germany (28%), and the UK (27%). In the UK and the Czech Republic, job scams saw a 13% spike compared to 2024, emphasising the constantly evolving nature of authorised fraud.

Investment scams
Investment scams were reported at higher than average rates in Sweden (13%), Portugal (12%), Lithuania (11%), and Austria (11%).

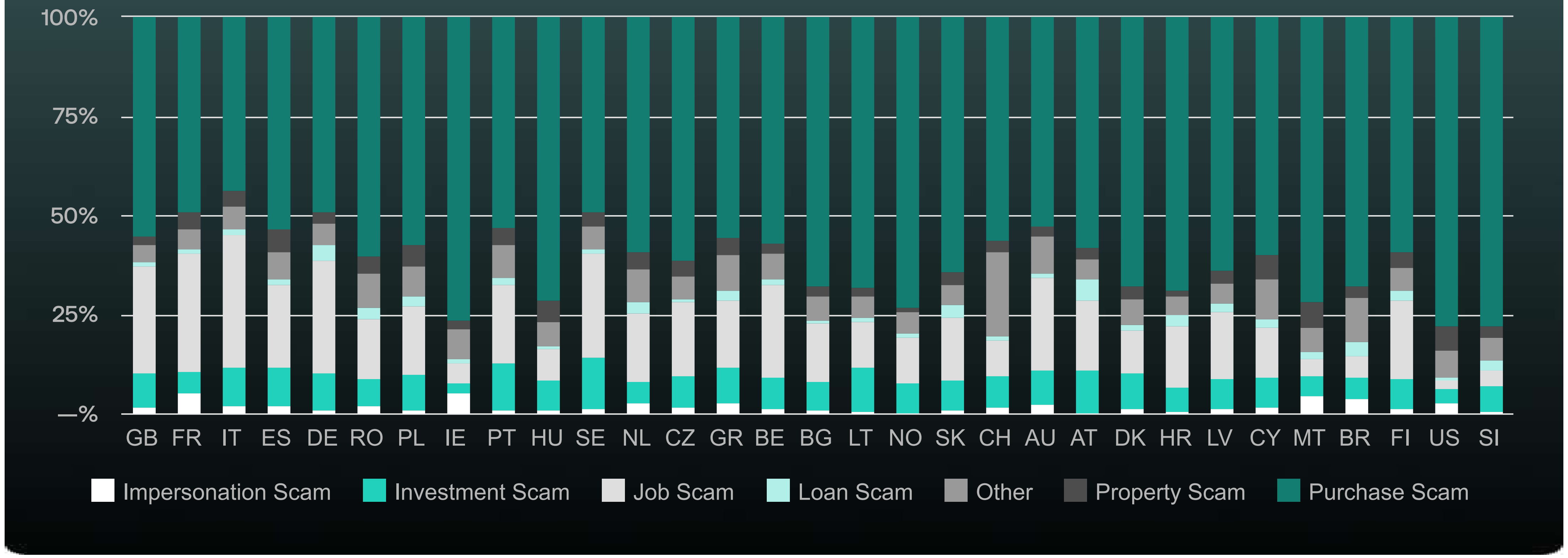
APP scam origin platform by % country

Exhibit 8



APP scam type by country

Exhibit 9



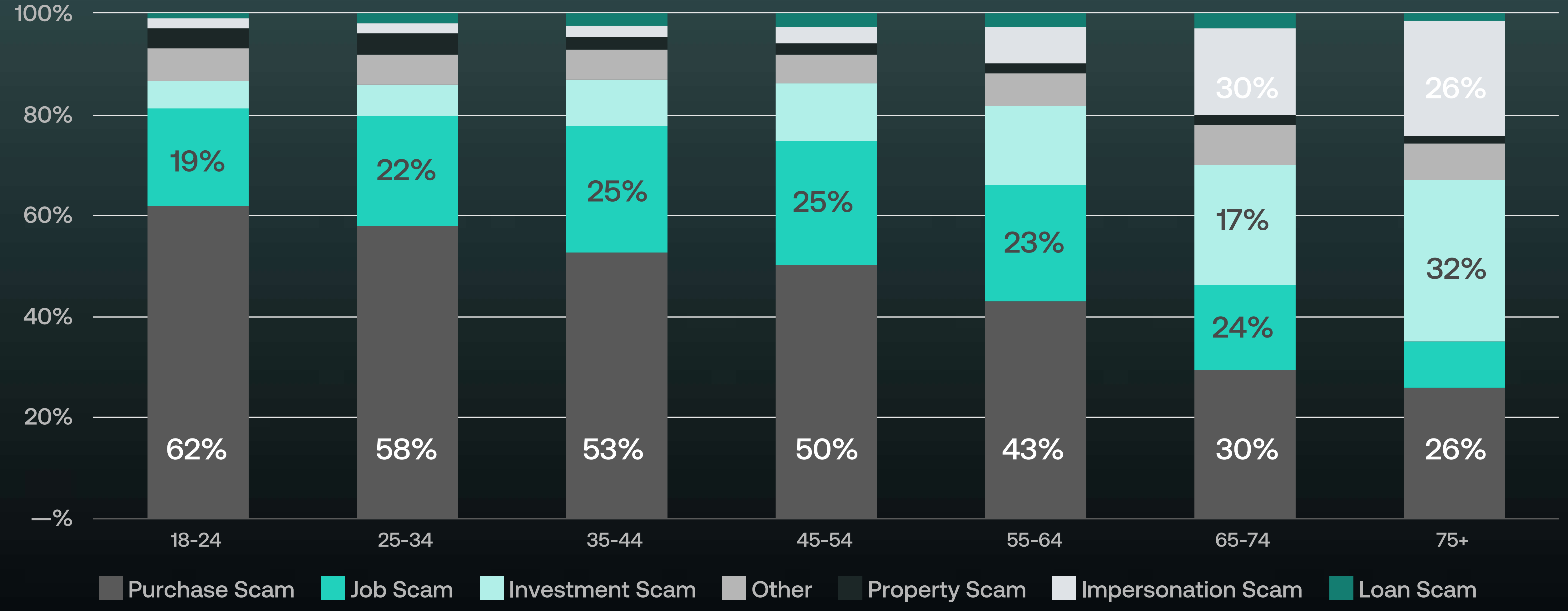
Fraud origination by age group

When looking at average losses per victim, customers over 35 lose 2.5x that of customers aged 18-34 to APP fraud. However, digging deeper reveals some important trends in the types of scams customers tend to fall for, which are vital for informing our fraud detection and prevention systems that alert and block these kinds of fraud.

The data also shows that scammers target younger customers with lower cost, higher volume purchase scams, and the opposite is true for elderly customers. Those over 65 are impacted 5-10 times as often as 18-24 year olds with impersonation and investment scams.

Distribution of APP scams by % age group

Exhibit 10



How to identify a scam

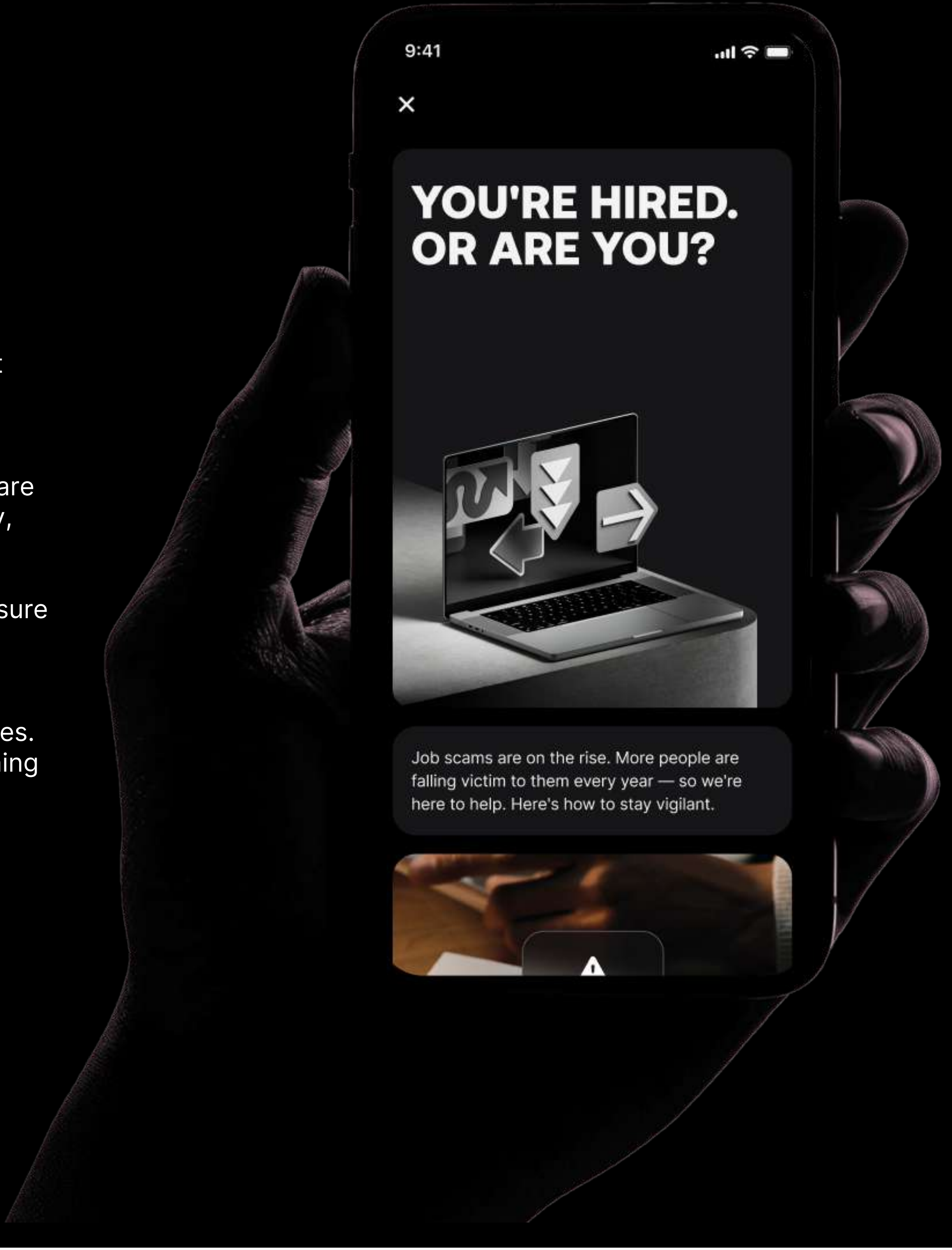
Revolut continues to educate customers by providing valuable information that helps them remain vigilant.

The data continues to indicate that a significant percentage of scams are initiated through social media, where users, often unknowingly, share sensitive personal information directly with scammers and are socially engineered to authorise payments

This growing trend highlights the need for all consumers to be vigilant and knowledgeable about the tactics fraudsters employ - such as impersonation, phishing, and fake investment schemes. By being aware of these strategies, consumers can better protect their financial assets and personal information, ultimately reducing the risk of falling victim to scams that rely on manipulation and deception.

Scammers often use tricks to get people to share their personal information or move their money, such as:

- Urgent requests. Scammers might pressure customers for immediate action, or ask them to keep things secret.
- Suspicious links, emails, or text messages. Customers need to double-check anything that seems odd or unfamiliar.

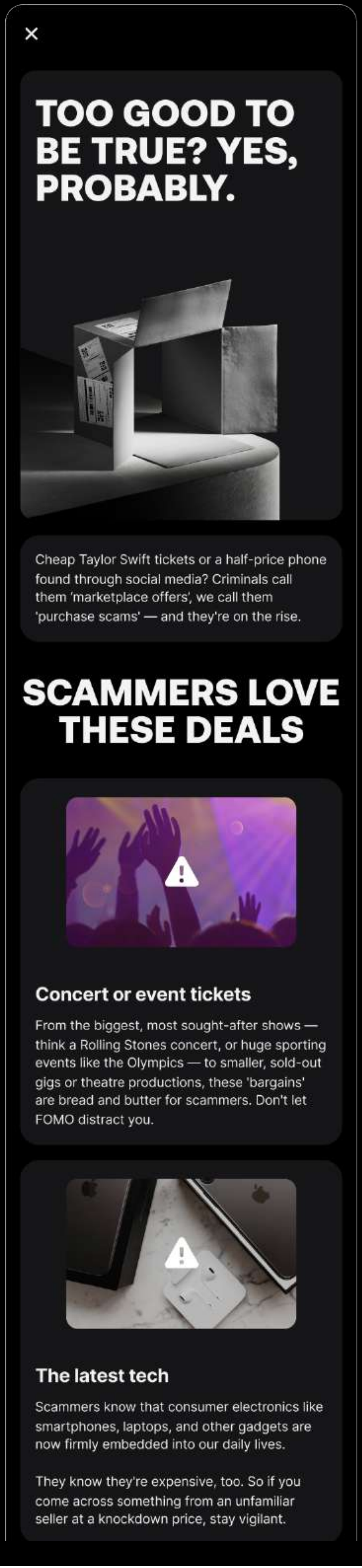


9:41

✕

YOU'RE HIRED. OR ARE YOU?

Job scams are on the rise. More people are falling victim to them every year — so we're here to help. Here's how to stay vigilant.



✕

TOO GOOD TO BE TRUE? YES, PROBABLY.

Cheap Taylor Swift tickets or a half-price phone found through social media? Criminals call them 'marketplace offers', we call them 'purchase scams' — and they're on the rise.

SCAMMERS LOVE THESE DEALS

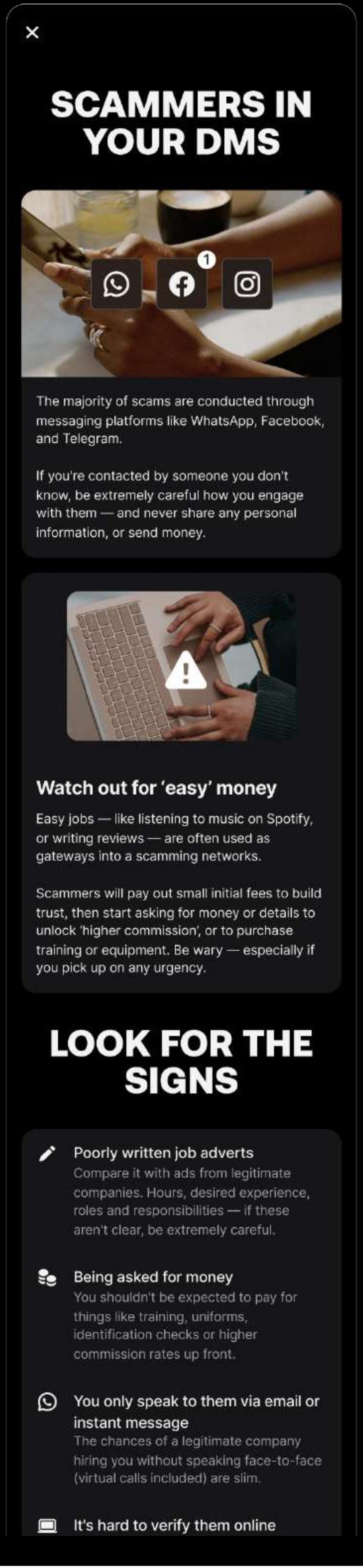
Concert or event tickets

From the biggest, most sought-after shows — think a Rolling Stones concert, or huge sporting events like the Olympics — to smaller, sold-out gigs or theatre productions, these 'bargains' are bread and butter for scammers. Don't let FOMO distract you.

The latest tech

Scammers know that consumer electronics like smartphones, laptops, and other gadgets are now firmly embedded into our daily lives.

They know they're expensive, too. So if you come across something from an unfamiliar seller at a knockdown price, stay vigilant.



✕

SCAMMERS IN YOUR DMS

The majority of scams are conducted through messaging platforms like WhatsApp, Facebook, and Telegram.

If you're contacted by someone you don't know, be extremely careful how you engage with them — and never share any personal information, or send money.

Watch out for 'easy' money

Easy jobs — like listening to music on Spotify, or writing reviews — are often used as gateways into a scamming networks.

Scammers will pay out small initial fees to build trust, then start asking for money or details to unlock 'higher commission', or to purchase training or equipment. Be wary — especially if you pick up on any urgency.

LOOK FOR THE SIGNS

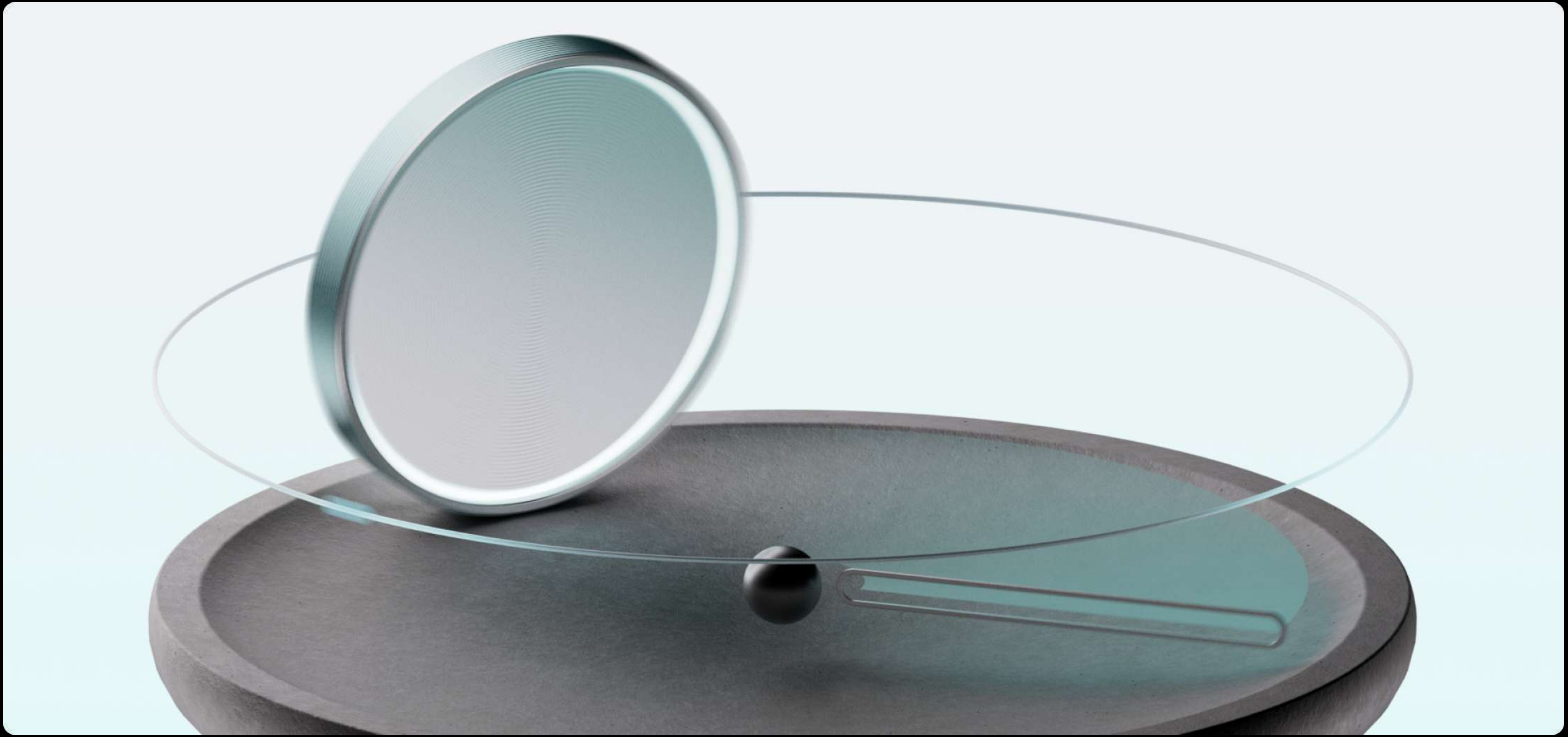
Poorly written job adverts
Compare it with ads from legitimate companies. Hours, desired experience, roles and responsibilities — if these aren't clear, be extremely careful.

Being asked for money
You shouldn't be expected to pay for things like training, uniforms, identification checks or higher commission rates up front.

You only speak to them via email or instant message
The chances of a legitimate company hiring you without speaking face-to-face (virtual calls included) are slim.

It's hard to verify them online

Unauthorised fraud deep dive: global overview



Unauthorised Fraud

Unauthorised fraud occurs when individuals unlawfully access another person's money, sensitive information, or assets by impersonating them. This form of fraud involves gaining unauthorised access to personal details, which may then be used to take over accounts, initiate unauthorised payments, or apply for credit cards in the victim's name.

Building upon our understanding of scammer tactics, it's crucial to delve further into the mechanisms behind unauthorised fraud.

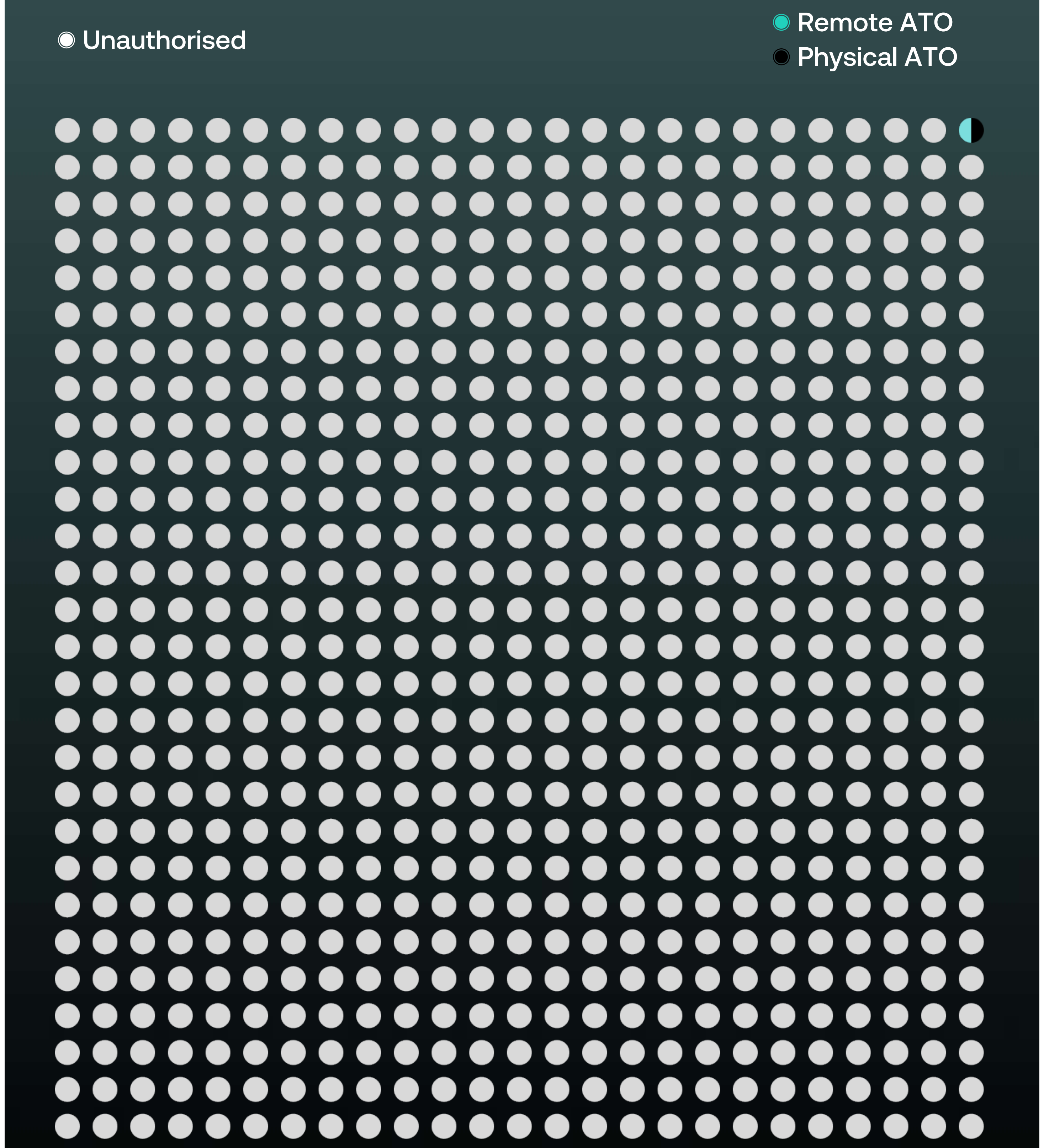
The data indicates that **unauthorised card fraud** remains the dominant form of attack, consistently accounting for over 99% of reported cases over 2025.

Preventative measures, such as Revolut’s virtual cards for single-use transactions, continue to play a significant role in mitigating the impact of these attacks.

The data also reveals a negligible presence of Remote ATO (Account Takeover) and Physical ATO incidents throughout the observed period. This suggests that robust security protocols, including multi-factor authentication, advanced fraud detection systems, and enhanced security products such as Wealth Protection are effectively minimizing these types of unauthorised access.

Unauthorised Card Fraud breakdown by type of fraud 2025

Exhibit 11



How Revolut is fighting fraud

Security Features

Protecting customers from fraud and financial crime remains a core priority for Revolut. We invest heavily in customer protection, and nearly 1/3 of Revolut's total global workforce now work in Financial Crime Prevention.

At the forefront of Revolut's security measures is its proprietary fraud detection system, employing cutting-edge machine learning and artificial intelligence methodologies. We monitor rapidly evolving trends in scammers' tactics and deploy innovative solutions designed to enhance customer protections and provide them with more control over their money.

We also reinforce these efforts with proactive customer communications, helping users recognise evolving scam tactics and take practical steps to stay protected. Together, these measures encourage customers to pause, reassess risks, and access support when it matters most.

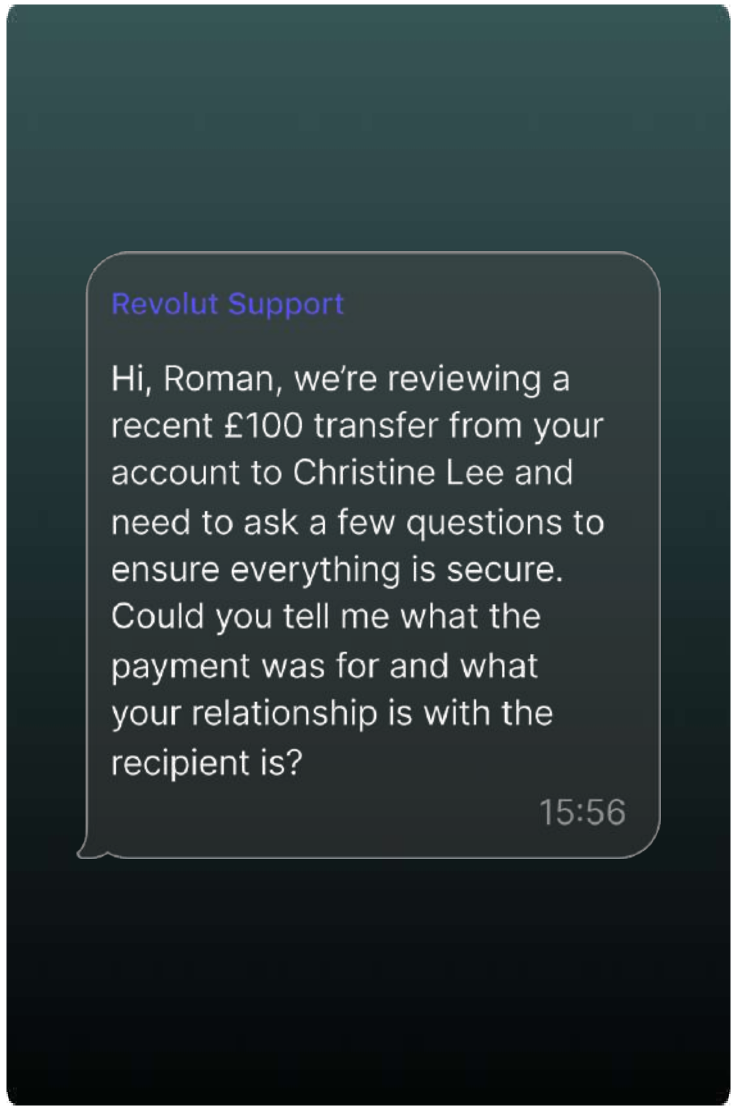
Every year Revolut introduces a number of new initiatives to combat increasingly sophisticated fraud threats. We continuously strengthen protections across the customer journey, combining smarter fraud monitoring with clearer, more timely interventions to disrupt scams at critical moments. This section sets out key elements of Revolut's Security Suite and Wealth Protection offering.

However, financial crime remains an industry-wide issue, and no one institution can tackle the issue alone. Staying ahead will require continued investment, innovation, and close collaboration across other banks, payments providers, social media platforms and telecoms networks.

Scam Buster

To further improve our scam intervention measures and break fraudsters' manipulative 'spells', Revolut has deployed a groundbreaking AI-powered chatbot designed to deliver context-enriched, targeted scam warnings to our customers.

The Scam Buster utilises conversational data to predict the likely scam type a customer is falling for, facilitate an interactive and dynamic conversation, and identify the most effective form of support our customers need to stop fraud in its tracks.



Revolut Support

Hi, Roman, we're reviewing a recent £100 transfer from your account to Christine Lee and need to ask a few questions to ensure everything is secure. Could you tell me what the payment was for and what your relationship is with the recipient is?

15:56

Transaction Limits

In order to provide customers with more flexibility and control over their money, whilst still offering additional layers of security, Revolut has developed a feature to allow customers to set their own daily transaction limits, requiring biometric authentication over their personalised limit. This means that, both for everyday spending and in the event of compromised cards or accounts, customers have more control over their money.

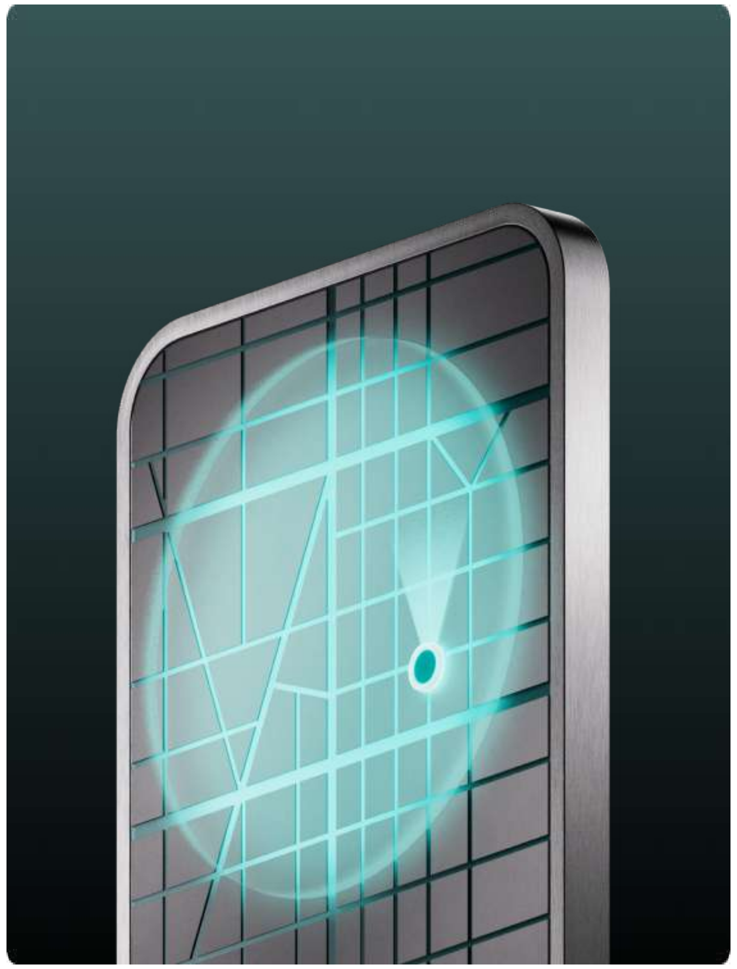
Wealth Protection

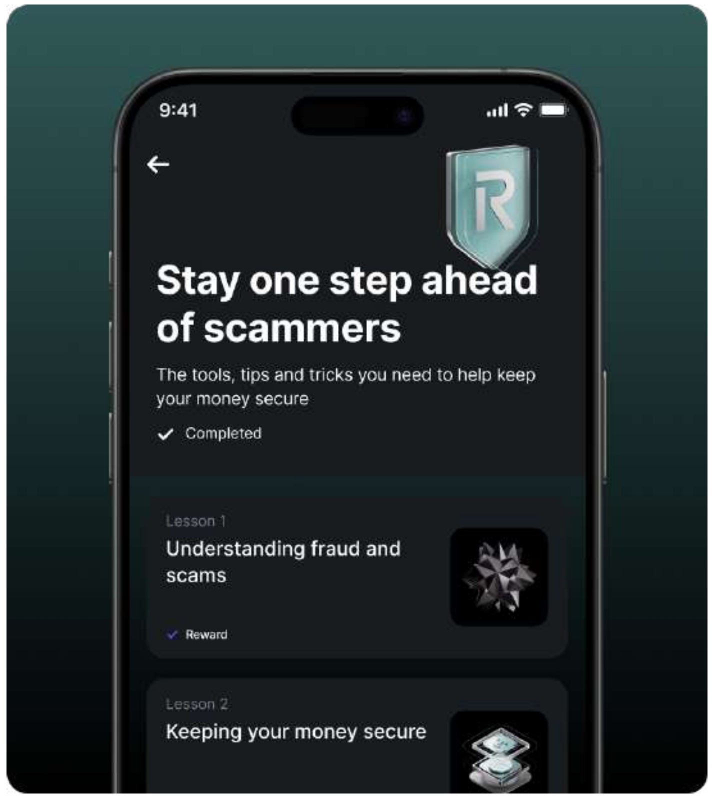
Revolut allows users to set up biometric authentication for withdrawals from their investments, as an extra layer of protection. Once enabled, all withdrawals from the following savings and investments will require selfie verification: Savings, Investments, Commodities, Personal Pockets, and crypto trades and transfers.

Street Mode

Criminals are becoming increasingly aggressive in their attempts to steal customer funds, and customers are becoming more vulnerable to 'transfer muggings', a type of theft where customers are forced to unlock their phone and transfer money to the thief. Street Mode tackles this growing problem by allowing users to set 'Trusted Locations' for their transaction limits. Outside of these areas, all transfers exceeding the limit will be subject to a one hour delay and second biometric authentication. This creates vital friction in the transfer process where theft can be prevented by stopping funds from being transferred under duress.

Street mode was recently recognised by 11:FS as the **Best Scam Prevention** tool for its ability to protect customers against real-world coercion and social engineering.





Stay one step ahead of scammers

The tools, tips and tricks you need to help keep your money secure

✓ Completed

Lesson 1
Understanding fraud and scams

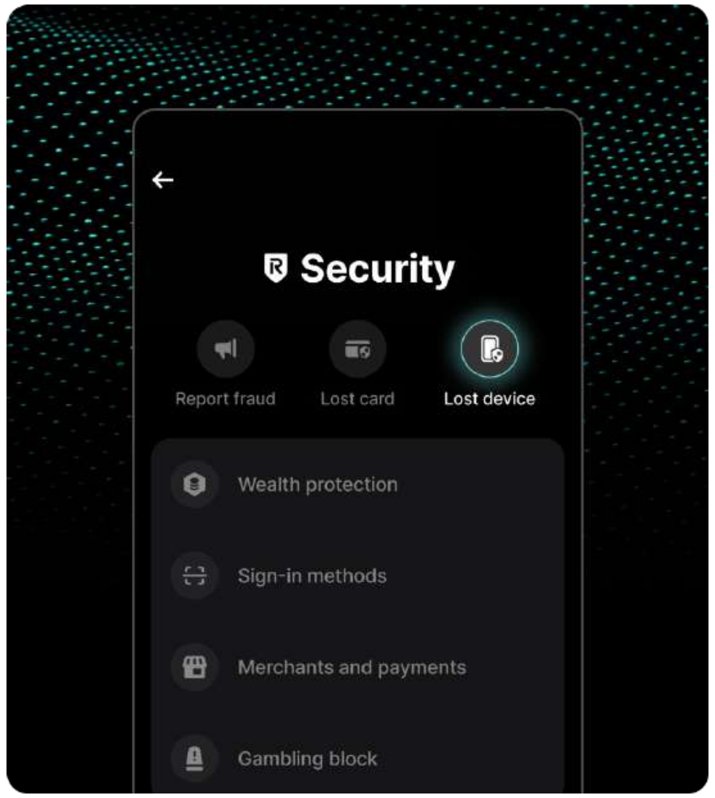
✓ Reward

Lesson 2
Keeping your money secure

Fraud Learn 2.0

Revolut's in-app Fraud Learn course empowers customers with the knowledge and tools necessary to stay one step ahead of malicious actors.

Customers can learn about the common trends in fraud and scams, and learn to recognise the warning signs of risky transactions and bad actors.



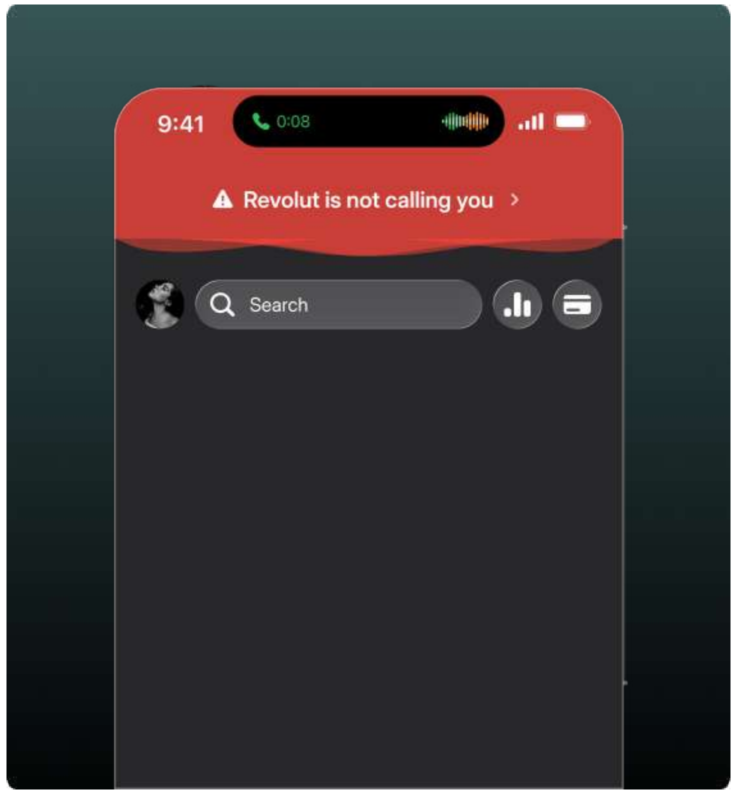
Lost device

Physical account takeover becomes an urgent and serious threat; acting fast after a device is lost or stolen is imperative to protecting customer's money.

In order to provide customers with the agency to act instantly and secure their account in an emergency, Revolut has developed a lost device feature, which allows customers to log out of all devices, both within the app and via the website. Customers will be able to lock down their account in minutes, from any device.

In-app voice call

In order to minimise the potential for phone call impersonation scams, which leaves customers vulnerable to scammers posing as bank employees or customer service representatives, Revolut has launched an in-app voice call feature, which provides customers with the peace of mind that the person on the other end of the line is a verified Revolut employee.

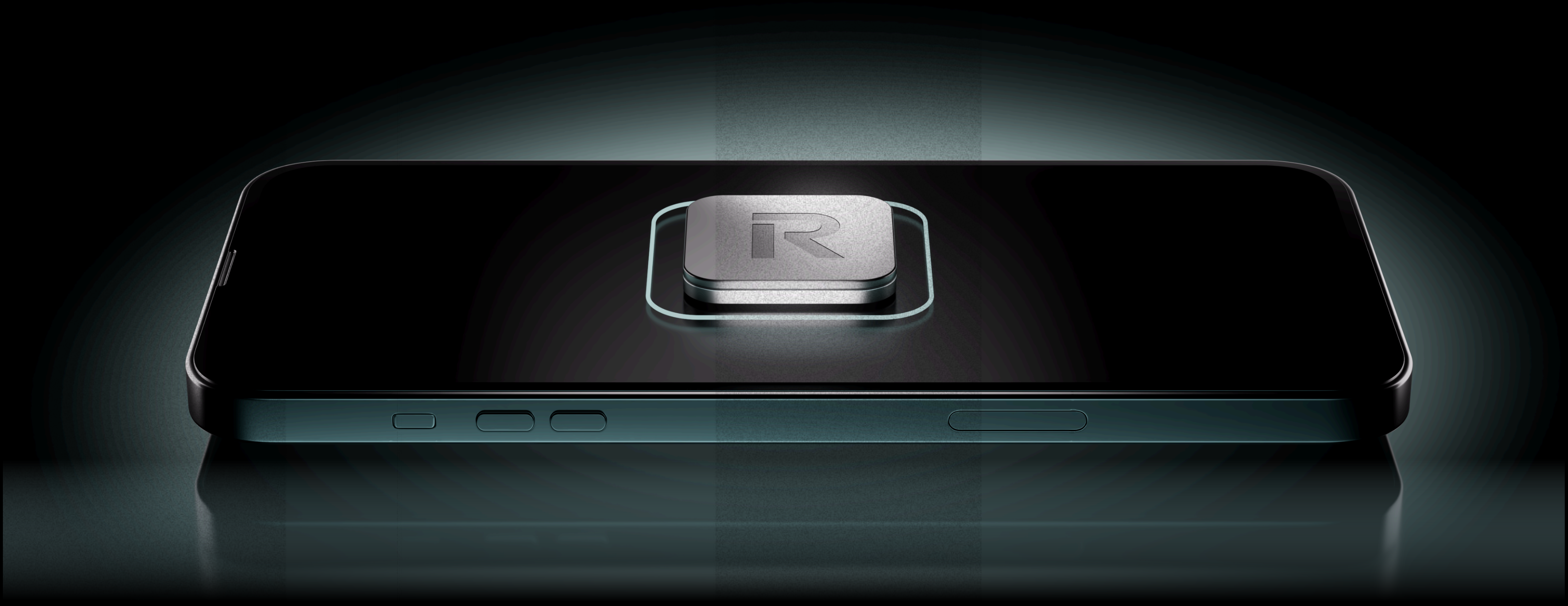


⚠ Revolut is not calling you ›

In-app call identification

To protect customers against the growing threat of call-based impersonation scams, driven by the proliferation of AI in scam calls, Revolut has launched a feature that automatically detects when users are on a call with a Revolut employee. If the call is genuine, customers will see confirmation that they are in contact with a legitimate agent. If Revolut cannot verify that the customer is on a legitimate call, a prominent warning message will be displayed in the app. Customers can tap the banner to be taken through an emergency fraud reporting flow, where they can proactively lock their account and disable their cards, securing their details and allowing Revolut to take action against the fraudster.

Conclusions



Conclusions

The findings in this report show that while fraudsters continue to refine their tactics, the underlying enablers remain largely unchanged: namely the unchecked presence of scams on social media and messaging platforms.

At Revolut, we confront these realities head-on using our rich real-time dataset. We analyse millions of transactions every day to understand how scams emerge, how they mutate, and where criminals are shifting next. By examining patterns across over 40 markets, we can distinguish between global trends and local nuances, allowing us to adapt safeguards market by market and intervene earlier in the scam lifecycle.

This data-led approach is not theoretical. It is delivering measurable results. In 2025 alone, we reduced our fraud rate by 31%, and by around 60% compared with the start of 2024, despite facing a worsening scam environment. These improvements are driven by continuous investment in advanced machine learning, behavioural analytics, and consumer-first security features such as biometric protections, call detection, and Street Mode.

But even the most advanced bank-level controls cannot stop scams that originate upstream. The majority of authorised fraud begins with contact on social media, messaging platforms, or online marketplaces. That is why no single company, sector, or regulator can solve this problem alone.

Banks can block payments. But platforms have the power to stop scams before the first message is ever sent.

If we are serious about protecting consumers, we must move beyond fragmented efforts and towards a truly unified, intelligence-led response. That means faster and deeper data-sharing between financial institutions.

It means stronger partnerships with law enforcement to disrupt organised criminal networks at scale. And it means social media and messaging platforms taking far greater responsibility for detecting, removing, and preventing scam content on their services.

The opportunity is significant. The intelligence collectively held across the industry could transform our ability to predict, prevent and dismantle fraud ecosystems.

Fraud is an ecosystem problem, and it requires an ecosystem solution.

Today's data makes one thing clear. While the threat is growing, and tactics are changing - so too are our capabilities. With the right level of cooperation, transparency, and shared accountability, we can move from reacting to scams after harm occurs, to preventing them at source.

Revolut is committed to leading that shift. We will continue to invest heavily in people, technology and partnerships. We will continue to share insights openly with industry and policymakers. And we will continue to push for a model where consumer protection is not determined by which app a criminal chooses to use, but by a collective system designed to shut them down.

The choice before us is stark: work in silos and allow criminals to exploit the gaps between us, or work together and close those gaps for good.

Revolut Group Holdings Ltd
Registered number: 12743269