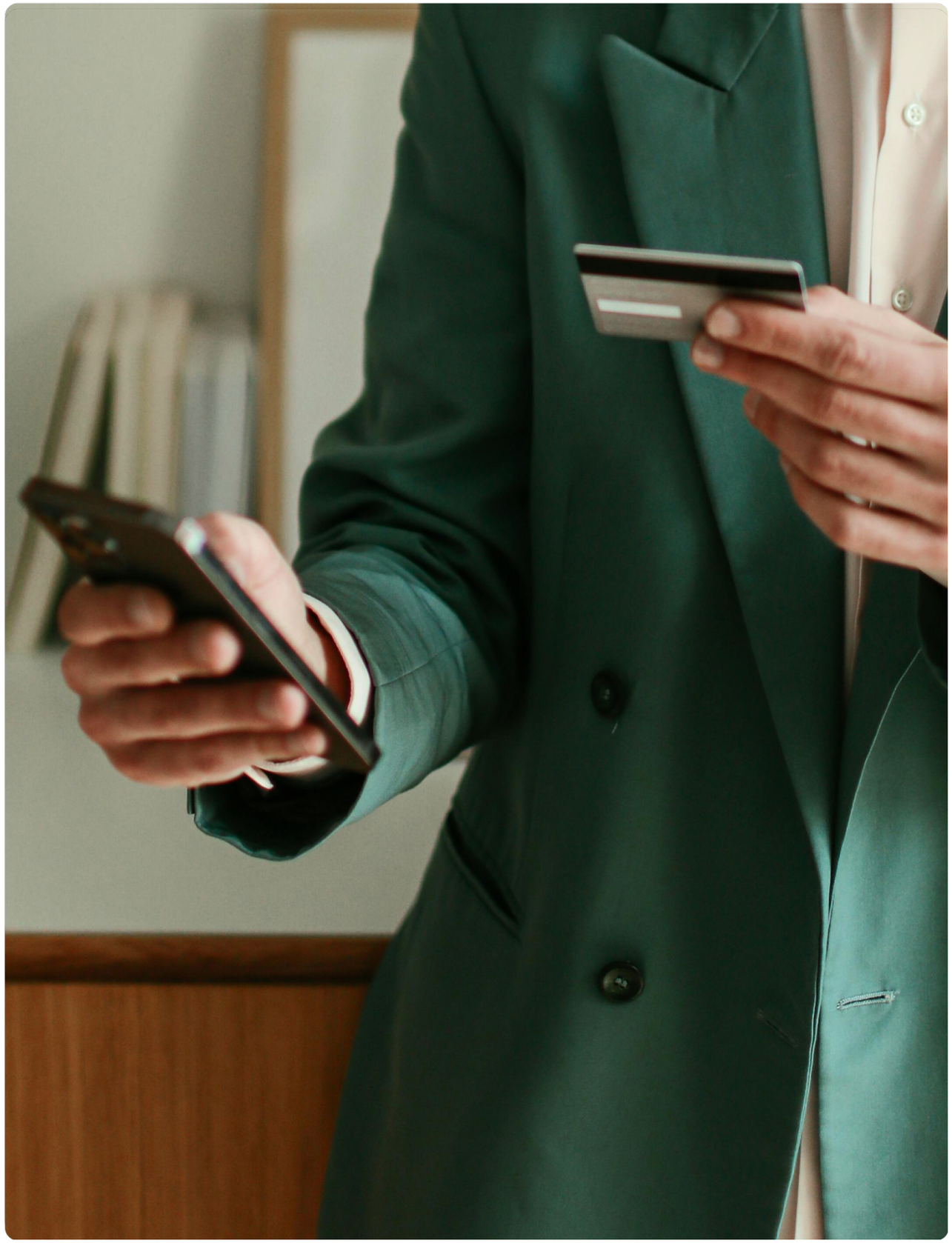
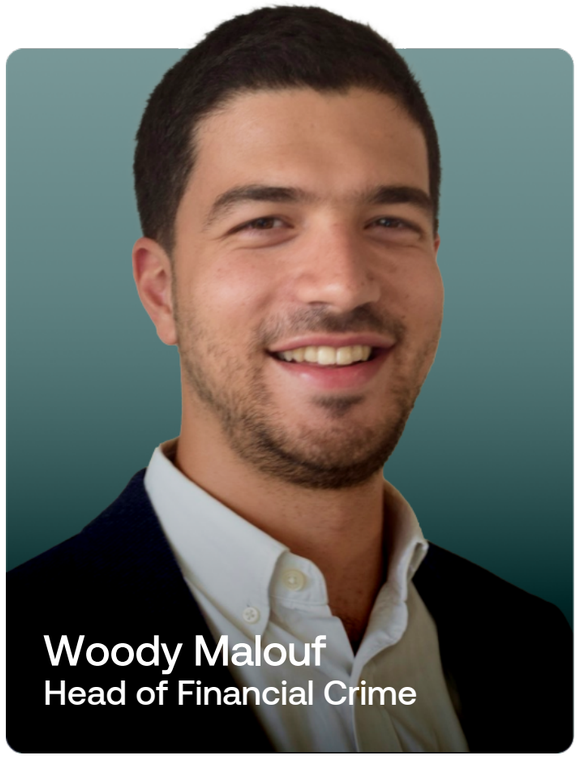
Revolut

Consumer Security and Financial Crime Report H2’24



Revolut Group Holdings Ltd
Registered number: 12743269



Woody Malouf, Head of Financial Crime at Revolut, on the third edition of our Consumer Security and Financial Crime Report H2'24

Fraud is a relentless and pervasive threat, impacting individuals and businesses across the globe on a daily basis. The criminals behind these schemes are constantly evolving their tactics to exploit vulnerabilities, and their actions demand vigilance and decisive action.

At Revolut, we take the industry-wide risk of customers being coerced by organised criminals incredibly seriously.

Our dedicated, 24/7 financial crime team prevented over £600 million in potential fraud in 2024 alone, and we invest heavily in cutting-edge security features; from in-app calls to combat impersonation scams to real-time AI fraud detection, transaction limits and biometric authentication.

This third edition of our Consumer Security and Financial Crime Report provides an updated analysis of this evolving landscape and outlines our ongoing measures to protect our customers. The aim of this report is simple; to shed light on the intricate web of scams and frauds which pose increasing threats to individuals around the globe.

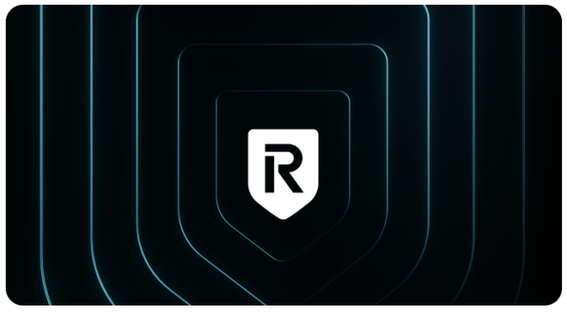
As before, this report details:

- the types of fraud that are most prevalent in the market
- the work Revolut has done to stop fraud and protect customers
- useful tips customers can use to protect themselves from these ruthless criminals

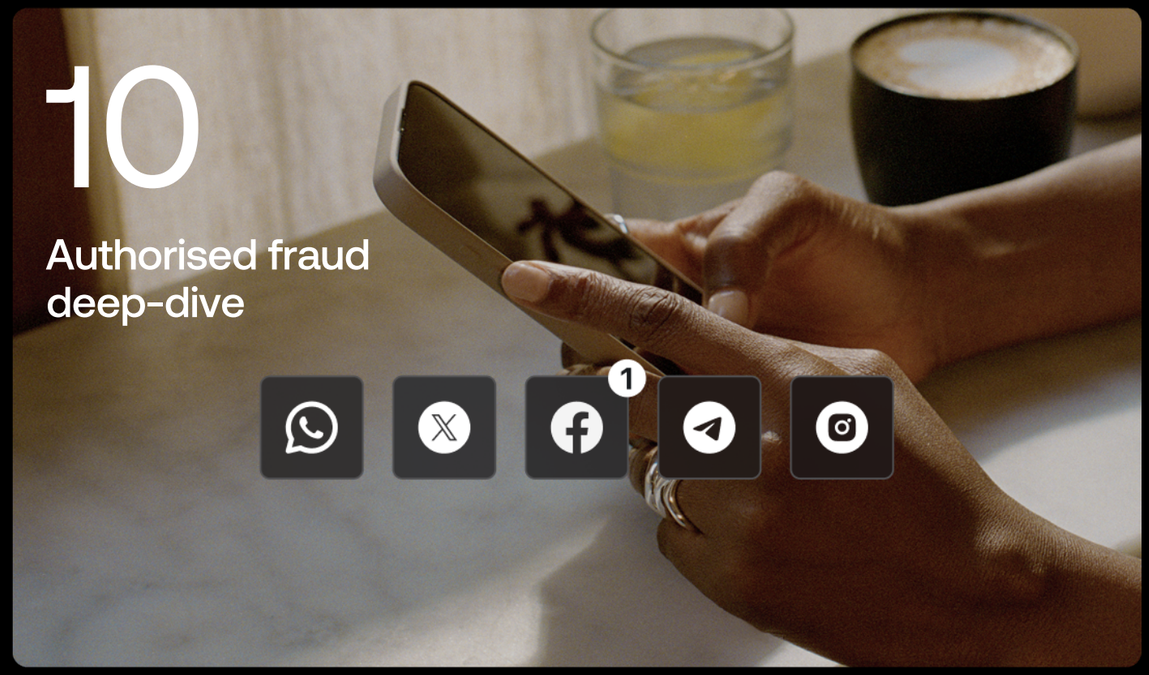
While our priority is to protect our customers and equip the industry with the insights needed to navigate these challenges, it is the **source** of these scams that demands urgent attention.

Over the past 24 months, we have observed a concerning trend: social media platforms, particularly Meta, remain a primary source of reported scams, yet remain reluctant to take comprehensive action.

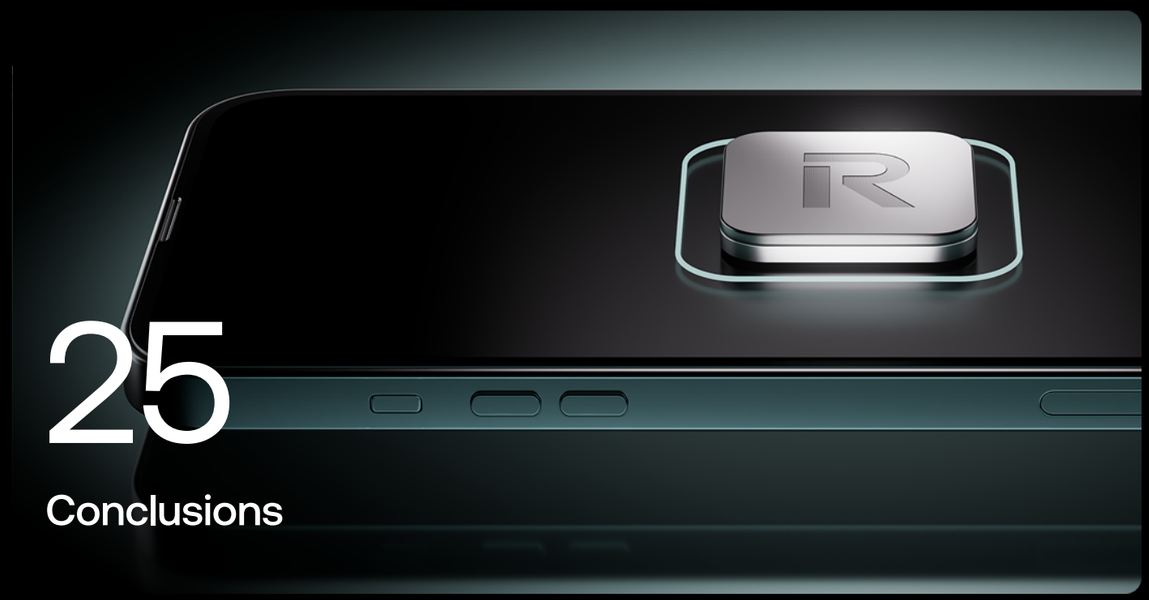
We have long advocated for proactive intervention, including more stringent verification processes for advertisers and content creators, robust AI-driven monitoring, and seamless collaboration with financial institutions and law enforcement. Additionally, we continue to push for commitments from social media companies to share reimbursement for victims of scams originating on their platforms. The current status quo remains unacceptable - we need immediate, decisive action, not empty promises.



Contents



22
How Revolut is fighting fraud



Methodology

Methodology

The findings in this report are based on anonymised data from the Revolut platform, spanning an 24-month period between 1 January 2023 - 31 December 2024.

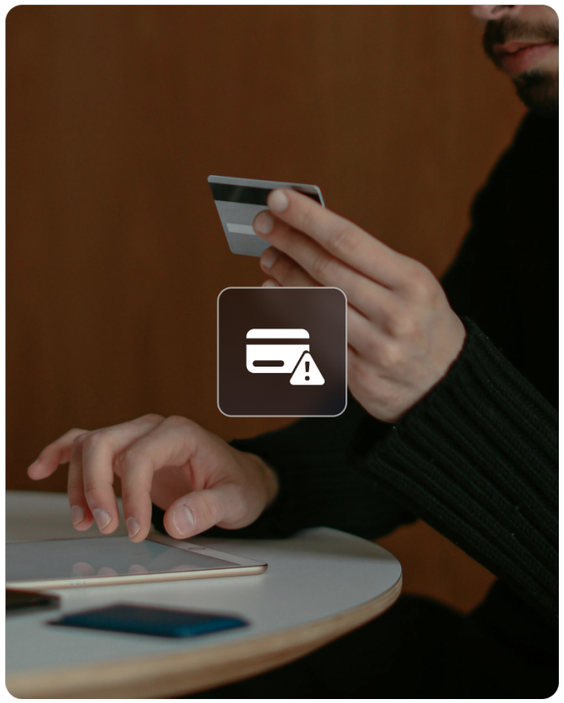
The data was taken from the following countries: UK, Ireland, France, Romania, Spain, Germany, Poland, Italy, The Netherlands, Hungary, Czech Republic, Greece, Portugal, Malta, Belgium, Lithuania, Belgium, Switzerland, Cyprus, Slovakia, Norway, Sweden, Latvia, Denmark, Croatia, Slovenia, Austria and Australia. This data set comprises reported fraudulent activity.

What is Fraud?

Fraud can be categorised into two main types: unauthorised fraud (or ‘fraud’) and authorised fraud (or a ‘scam’).

- **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.

- **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 (ATO):** Fraudsters gain access to a customer's account by obtaining security credentials and account information through digital means—such as phishing, malware, or social engineering—and then use a different device to make payments or transfer funds.
- **Physical Account Takeover (ATO)**: This occurs when a fraudster steals the customer's phone and security credentials, allowing them to access the account on the existing device and carry out unauthorized 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

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

Tax scams

Scammers pretend to be tax officials or law enforcement, making urgent calls about unpaid taxes. They might even imply that you could be arrested if you don't make the payment.

Purchase scams

Also known as the oldest trick in the book, and remains common practice. Fraudsters trick victims with fake websites or marketplace adverts that promise unrealistically low-priced products, that then aren't delivered. Rental scams are also considered a type of purchase scam, where fraudsters list fake rentals and ask for upfront deposits from potential renters.

Investment scams

Fraudsters 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.

Relationship or romance scam

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

Loan scams

Fraudsters 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.

Job scams

Scammers 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. Common tactics include:

- asking people to pay upfront for paid training, administration, and setup fees, or to purchase required equipment, such as a laptop or phone.
- offering a small commission for completing simple tasks and then encouraging the victim to deposit higher-value funds to take advantage of time-limited increases in commission.

Invoice scams

Also known as mandate fraud, this is when fraudsters pose as a subscription service, merchant, or service provider, and tell you the payment information has changed. They may use fake invoices to trick you into making a payment to their accounts. This type of fraud typically only comes to light when the genuine merchant or service seeks payment.

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 2023 & 2024, unless specified otherwise.

In the first half of 2024 in the UK, criminals stole £571.7 million through unauthorised and authorised fraud[1] according to UK Finance. Even with increased industry-wide efforts to protect consumers, the financial landscape is constantly evolving, and with it, the methods employed by fraudsters.

Our data reveals that unauthorised fraud still constitutes the majority of fraud cases, now at 60%, while authorised fraud accounts for 40%. This represents a slight shift from the distribution we observed at the end of H1 2024, where authorised fraud accounted for nearly 50% of total cases, as detailed in our previous report. The continued prevalence of unauthorised card and account takeover highlights the need for continuous investment in robust security systems to prevent this type of fraud.

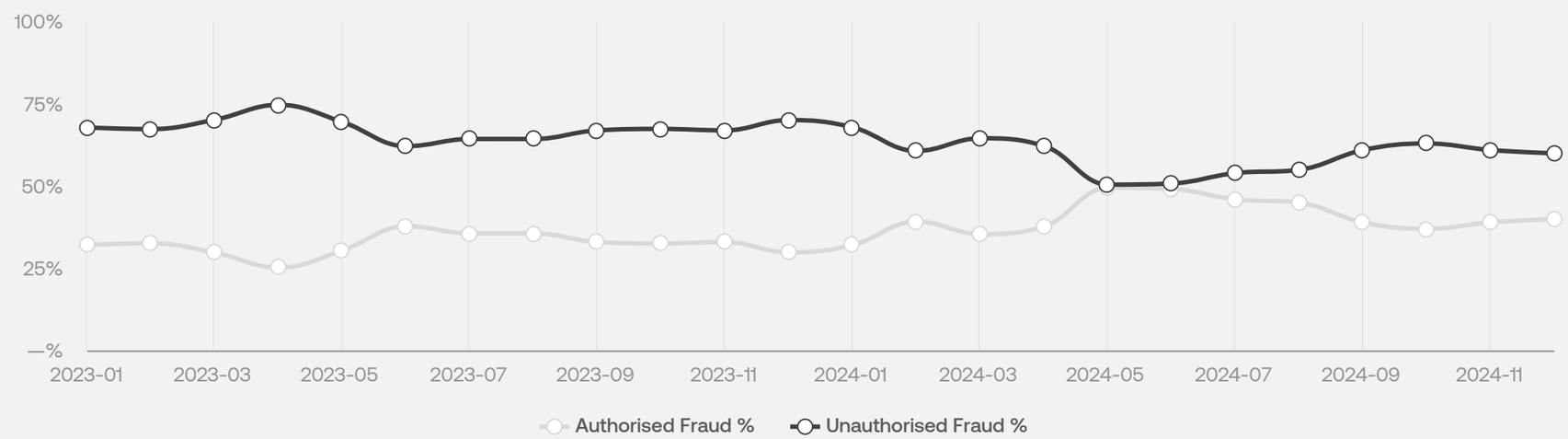
These scams, often executed through sophisticated social engineering tactics, trick individuals into authorising payments or sharing sensitive information. Fraudsters often impersonate trusted figures like bank officials, government agents, or service providers to gain victims' trust.

While the average loss per authorised fraud case remains higher than that of unauthorised fraud, we are committed to developing and implementing effective countermeasures for both types of fraud. In the previous report, we noted that the average loss from authorised fraud was 12 times greater than that from unauthorised fraud. Now, with the latest data, we observe that the average loss from authorised fraud is 14 times greater.

Financial institutions like Revolut are at the forefront of this battle, investing in advanced technology and education to protect consumers. By understanding the evolving nature of fraud and the tactics employed by scammers, we can empower individuals to make informed decisions and safeguard their financial well-being. In the following chapter, we will delve deeper into the specific types of authorised fraud, analyse their origins, and explore how Revolut is working to mitigate these risks.

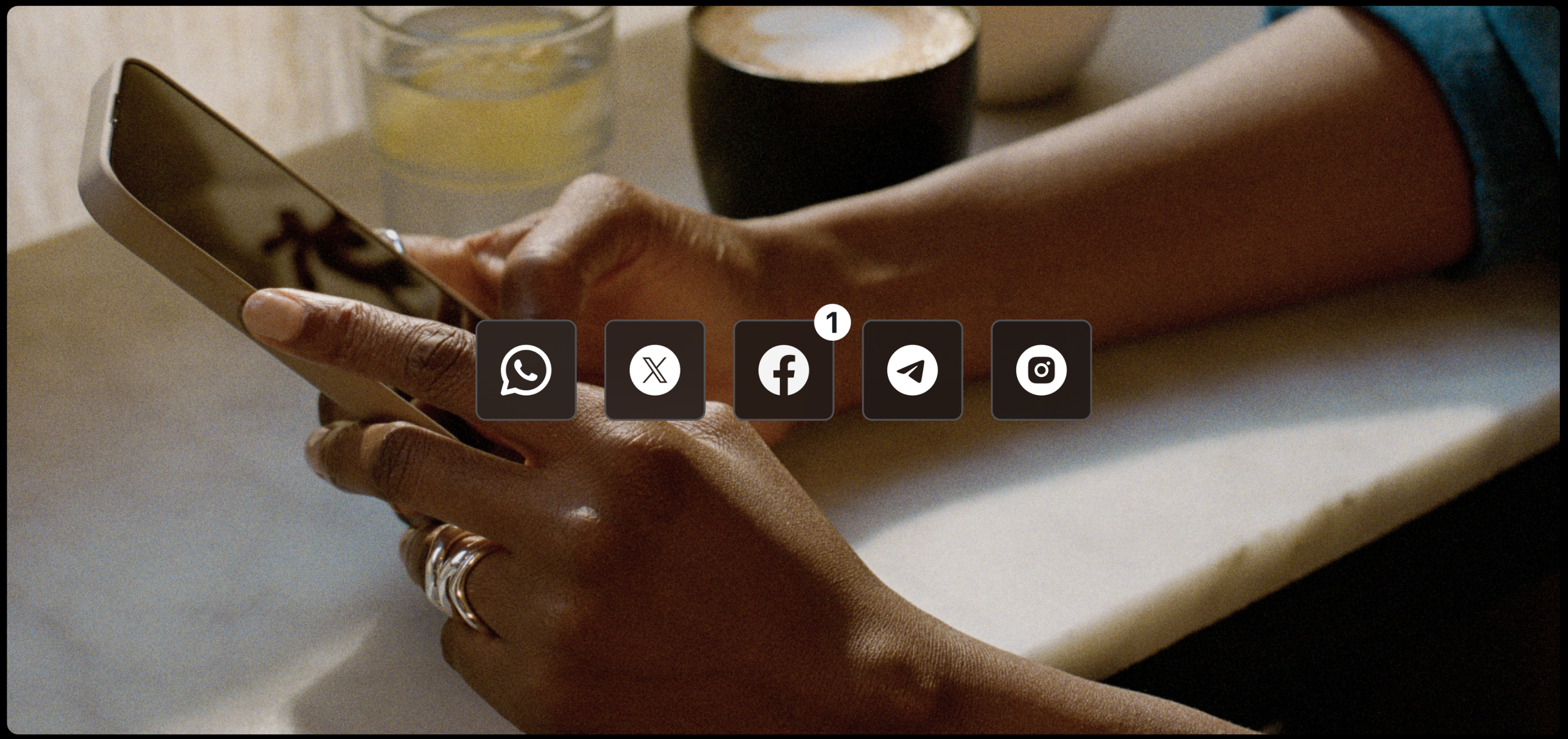
Exhibit 2 - Authorised Fraud vs. Unauthorised Fraud: average loss per victim H2'24

Exhibit 1 - Authorised Fraud vs. Unauthorised Fraud: distribution of victims (2023 - 2024)



[1] UK Finance

Authorised fraud deep-dive: global overview



Where does Authorised Fraud most commonly originate?

Meta Remains Dominant: Despite repeated calls for action, Meta platforms continue to be the leading source of authorised fraud, accounting for over 54% of cases in H2 2024. Within the Meta ecosystem, Facebook remains the leading individual platform for authorized fraud origination, accounting for ~28% of cases. WhatsApp cases also rose in this period by a concerning 67% in H2 vs H1'24. This reinforces the need for Meta to prioritize user safety and take concrete steps to reduce the prevalence of scams on its platforms.

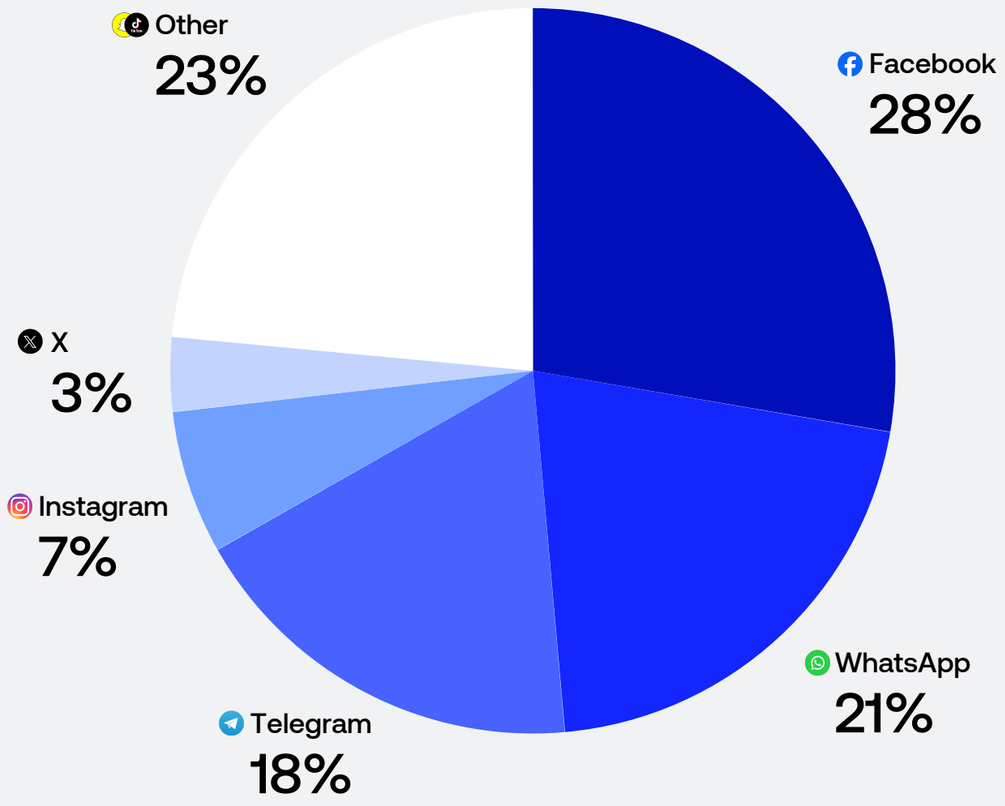
Telegram's Growing share: While Meta remains dominant, Telegram's share of authorized fraud origination has increased significantly, accounting for 18% of cases in H2 2024. Fraud originating on Telegram jumped by a staggering 121% in H2;

The data highlights, once again, that collective action is the only way to effectively tackle the root causes authorised fraud. Financial institutions, regulators, and social media platforms must work together to develop and implement effective prevention strategies to stop fraud at its source, starting with the most prevalent threats.

To further understand the nuances of purchase scams on these platforms, we'll now examine their breakdown by country and the source of fraud.

Meta remains dominant, marking the third consecutive reporting period where Meta has held this position

Exhibit 3 - Authorised fraud by source of origination H2'24 (% of total victims of Authorised Fraud)



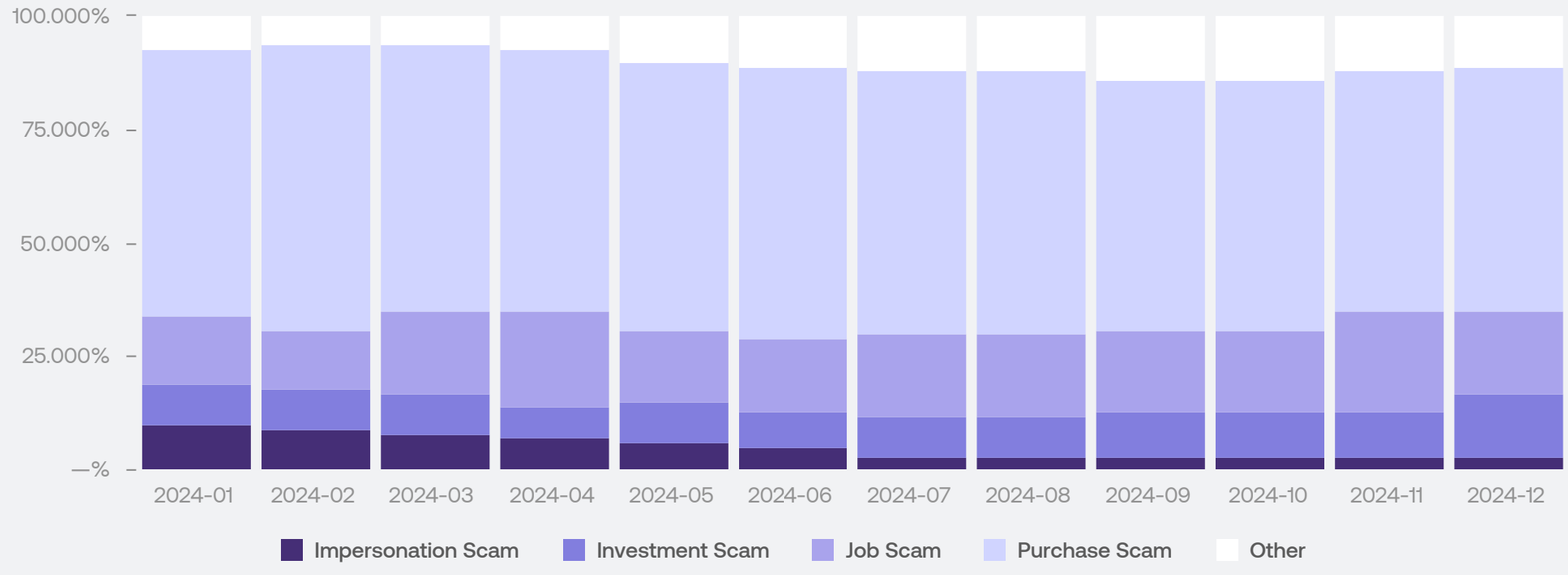
Which APP scams are most prevalent?

Despite the ever-changing nature of fraud, one thing remains constant: the prevalence of purchase scams. These scams, which exploit consumers' trust in online shopping and social media marketplaces, continue to be the most common type of authorized fraud. This aligns with our H1 2024 findings, where purchase scams accounted for 62% of all APP scams, representing a significant portion of cases. This highlights the persistent vulnerability of consumers to scams of this nature.

While purchase scams remain dominant, the data reveals other notable trends:

- **Job Scams**: The trend observed in H1'24 has continued in the second half of the year, affecting 20% of the total amount of APP fraud victims.
- **Investment Scams**: Fluctuating throughout the year, these have seen a significant overall increase, reaching 14% by year-end, almost doubling from 8% in early 2024. As with any substantial increase in fraud types, we are investigating the driving factors behind this change.
- **Impersonation Scams**: These have remained relatively stable, hovering around 4-10% throughout the reporting period.

Exhibit 4 - Purchase scam breakdown by source of Fraud - 2024



Top 3 types of APP Scams

56%

of APP cases were **Purchase Scams in H2'2024**

20%

of APP cases were **Job Scams in H2'2024**

10%

of APP cases were **Investment Scams in H2'2024**

While purchase scams dominate the overall landscape of authorized push payment (APP) fraud, a closer look at the distribution of scam types across different countries reveals interesting regional variations. Understanding these nuances is crucial information that Revolut uses for tailoring prevention strategies and educational initiatives to specific populations and their unique vulnerabilities.

Examining the data specific to each country, we can identify a number of key takeaways:

Purchase Scam Dominance

Purchase scams remain the most common type in most countries, with particularly high prevalence in Ireland (80%), Hungary (70%), Lithuania (70%), and the Czech Republic (68%). This highlights the consistent vulnerability of consumers to online shopping and social media marketplace fraud across all markets.

Job Scam Prevalence in Italy and France

Italy (IT) and France (FR) stand out as countries where job scams are highly prevalent, accounting for 52% and 28% of cases respectively. This highlights the need for continued targeted awareness campaigns and preventative measures in these countries which focus on employment-related scams.

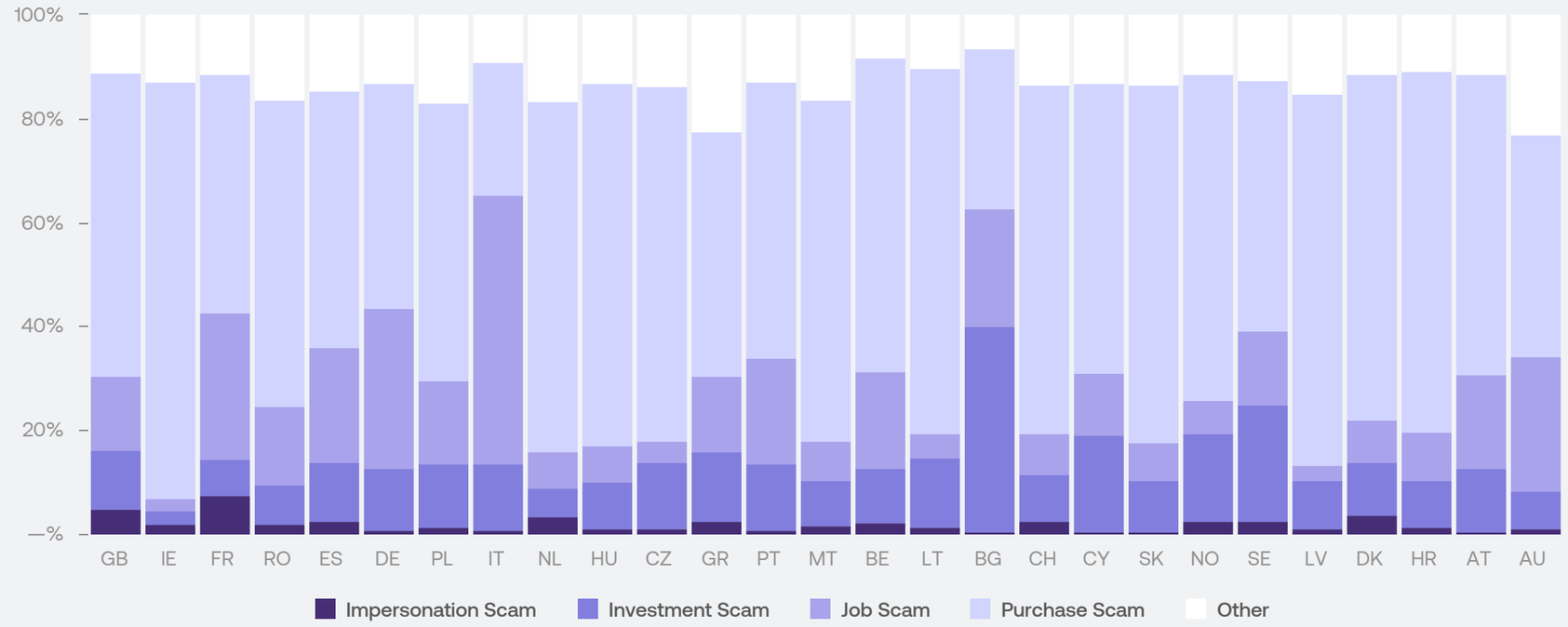
Investment Scams in Bulgaria and Sweden

Bulgaria (BG) and Sweden (SE) show a significantly higher proportion of investment scams (39% and 22%, respectively) compared to other countries.

As highlighted in Exhibit 2, authorised fraud, on average, results in losses 14 times greater than unauthorised fraud. Identifying the preferred channels scammers use to deceive consumers is critical in the fight against fraudsters. However, as we will examine in the next section of the report, tackling this issue effectively requires more than just vigilance from financial institutions—it calls for a collaborative approach.

It is important to recognise that trends in fraudulent activity differ depending on the country, and each region requires careful analysis in order to develop targeted approaches when combatting these scams.

◉ Exhibit 5 - Authorised Fraud APP breakdown by type of scam - H2'24



Purchase scams

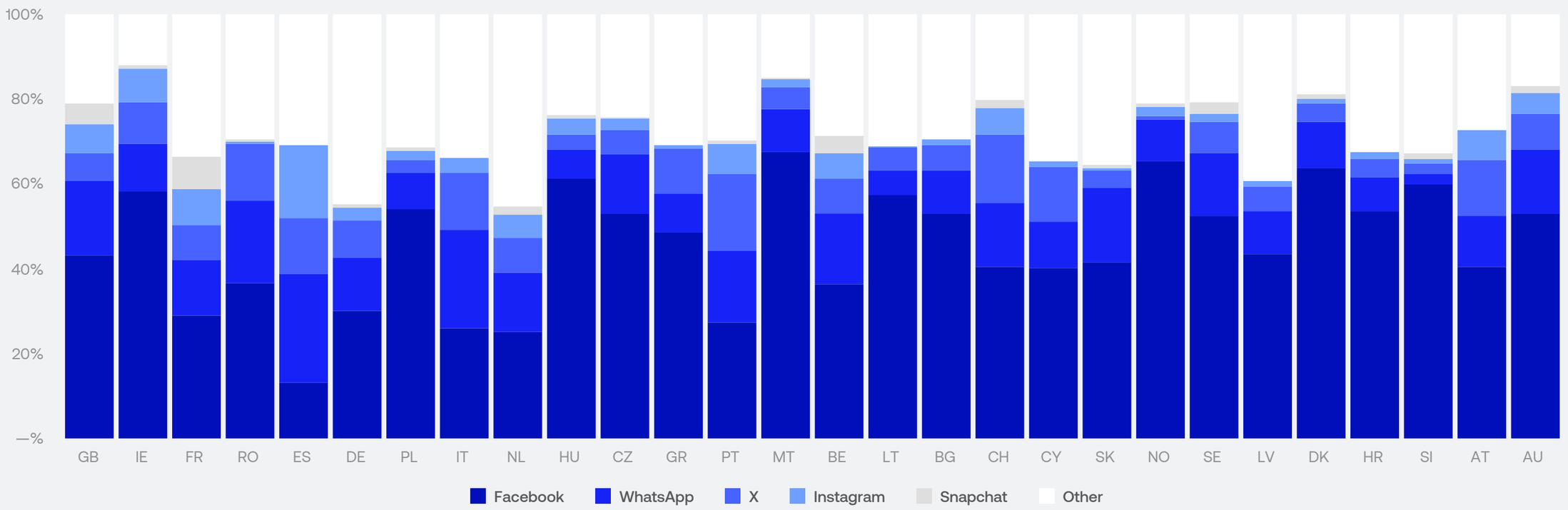
As evidenced by Exhibit 5, Facebook remains a significant source of purchase scams across all markets. Facebook's global reach and thriving second-hand marketplace have made it an ideal environment for fraudsters to exploit trust and convenience in online shopping. In countries like Ireland (IE), Malta (MT), and Hungary (HU), over 60% of reported purchase scams originate on Facebook. This highlights more than ever the need for Meta to enhance security measures on its platforms; in the UK alone, Facebook still accounts for over 40% of total purchase scams.

In Romania (RO), Italy (IT), Greece (GR) and France (FR), there is also a higher frequency of purchase scams on Instagram and WhatsApp when compared to other countries.

WhatsApp is emerging as a key platform for hosting purchase scams in several regions. In Spain (ES) and Italy, WhatsApp surpasses Facebook as the leading source platform, hosting over 25% of scams. Encrypted messaging capabilities, including those leveraged by WhatsApp and Telegram, provide a sense of privacy and promote consumer trust, which fraudsters readily exploit.

On the other hand, Spain presents an interesting deviation from the mean. Unlike the global trend, Spain is the only country in the data set where X, rather than Meta-owned platforms, is the predominant host, accounting for more than 10% of purchase scams.

◉ Exhibit 6 - Purchase scam breakdown by source of Fraud - H2'24



Deep dive: Ticket scams

The second half of 2024 was defined by major global events, from international sporting championships to world tours, uniting millions of fans around the globe. Unfortunately, they also provided fertile ground for scammers to prey on individuals eager to secure tickets. Ticket scam represented ~19% of total purchase scams in 202

The data demonstrates a troubling surge in ticket scams, particularly targeting younger demographics. As the graph clearly illustrates, individuals aged 17-24, and 25-34 accounted for the vast majority of reported cases, representing a staggering 74% of cases combined. This period coincided with the lead-up to several popular events as well as the Christmas gift buying season. When Revolut became aware of the sharp rise in scams, we alerted customers in high-risk areas through targeted educational communications.

Scammers likely capitalised on the heightened demand for tickets, employing tactics like fake social media giveaways, phishing emails mimicking official ticketing platforms, and fraudulent resale websites. This suggests that even highly digitally literate demographics are vulnerable—likely due to increasingly sophisticated phishing techniques designed to exploit eager fans by manipulating their sense of urgency.

Revolut continues to be diligent in communicating these risks to both consumers and the media.

Mirroring the overall pattern observed for purchase scams, the majority of ticket scam fraud is reported to have originated on Facebook.

In H2'24, almost 60% of total ticket scams happened through Facebook alone. X followed, hosting 18% of reported cases, and WhatsApp, Instagram, and Telegram collectively accounted for just over 15% of reported scams; while these platforms are less dominant, they still present a notable risk for consumers.

Exhibit 7 - # of Victims of Ticket scams per age group H2'24:

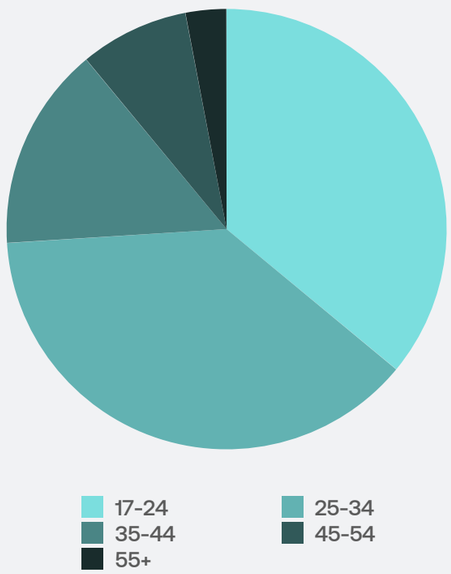
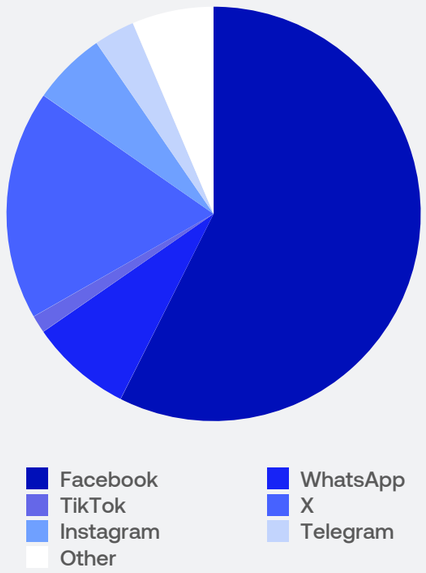
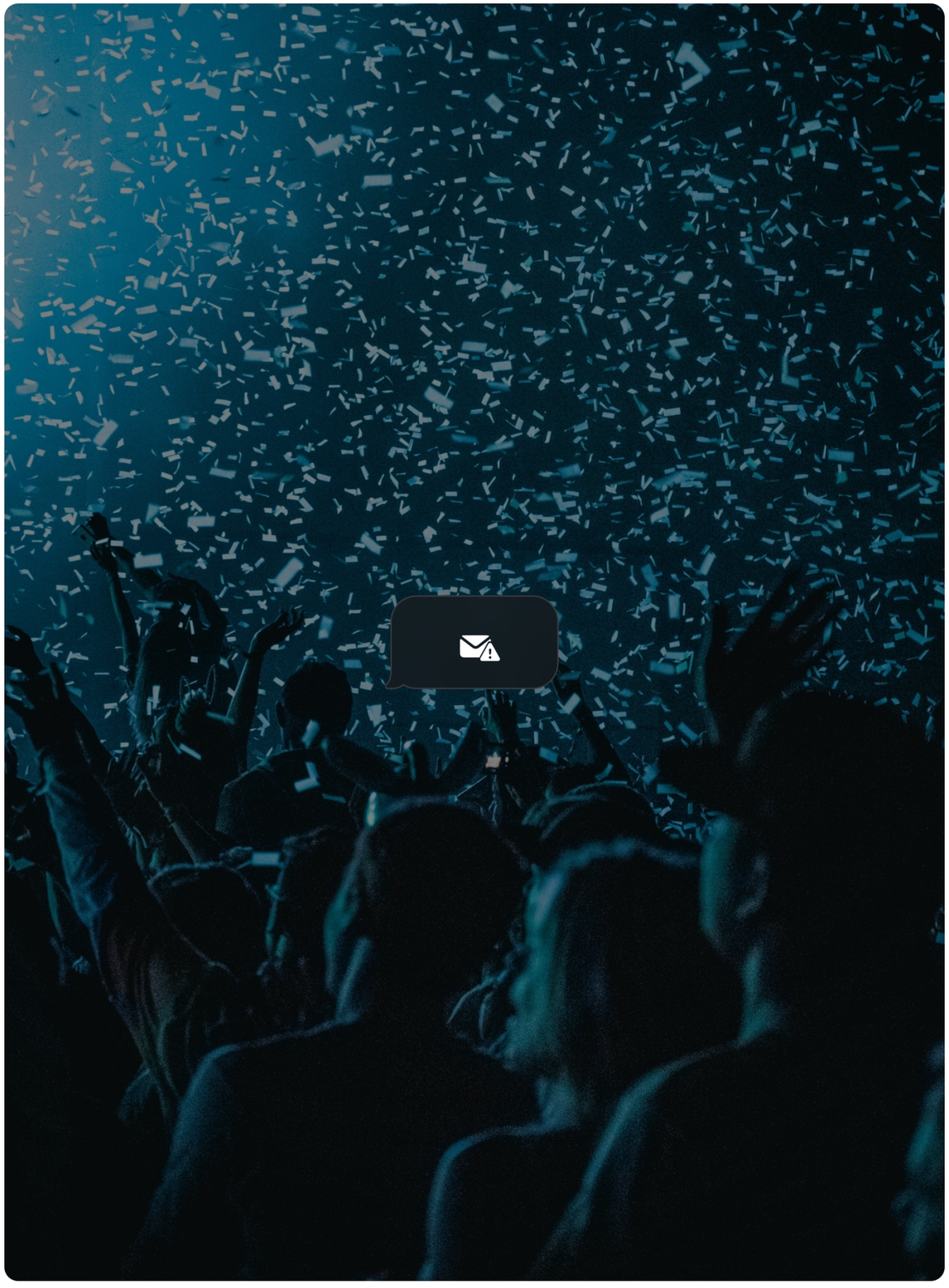


Exhibit 8 - # of Victims of Ticket scams by platform:





Job scams

When comparing the frequency and prevalence of job scams compared to purchase scams, there's one key differentiator to note — the hosting platform.

Examining the landscape of job scams reveals some distinct trends in platform usage. While Facebook is the number one source of purchase scams, job scams show a different pattern.

Telegram again emerges as a prominent platform for job scams across a significant number of countries, highlighting its appeal as a platform for fraudsters to exploit job seekers. WhatsApp also plays a crucial role in facilitating job scams in several countries. Platform preference for job scams also varies by region, emphasising the importance of tailoring prevention strategies to address the specific platforms used by fraudsters in different areas.

WhatsApp's prevalence

In countries including Great Britain (GB), Austria (AT), Czech Republic (CZ), Ireland (IE), Switzerland (CH), Denmark (DK), Sweden (SE), and Lithuania (LT), WhatsApp is commonly used by fraudsters to commit job scams. This highlights the exploitation of widely used messaging platforms for fraudulent purposes.

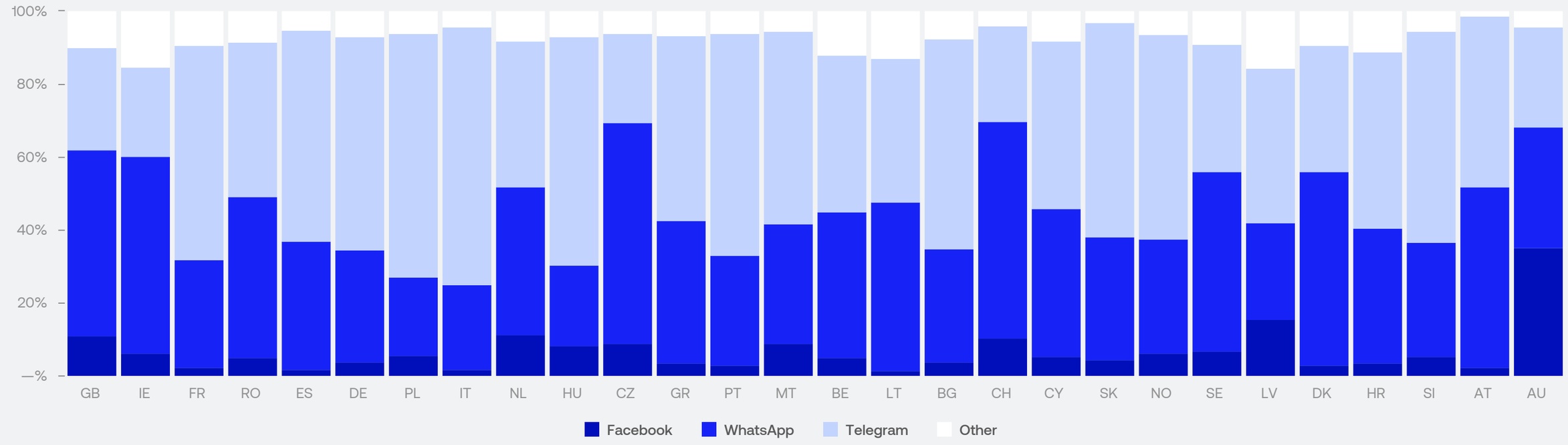
Telegram's dominance

Telegram appears to be the preferred platform for job scammers in France (FR), Poland (PL), Italy (IT), Portugal (PT), Hungary (HU), Slovakia (SK), Bulgaria (BG), Greece (GR), Slovenia (SI) and Cyprus (CY). The platform's group messaging features, such as public channels, likely facilitate the rapid distribution of fraudulent job offers.

Australia (AU) stands out

Australia was the only market where Facebook and WhatsApp share an almost equal proportion of job scam activity, suggesting fraudsters are leveraging both social media and messaging platforms with similar frequency to target vulnerable job seekers.

Exhibit 9 - Job scam breakdown by source of Fraud H2'24



Investment scams

Telegram's Prominence

Telegram emerges as a key platform for investment scams in several countries, including Australia (80%), Germany (60%), Hungary (47%), Spain (40%), and Romania (39%). This highlights Telegram's role in facilitating fraudulent investment schemes, likely due to features which support the easy dissemination of information at scale.

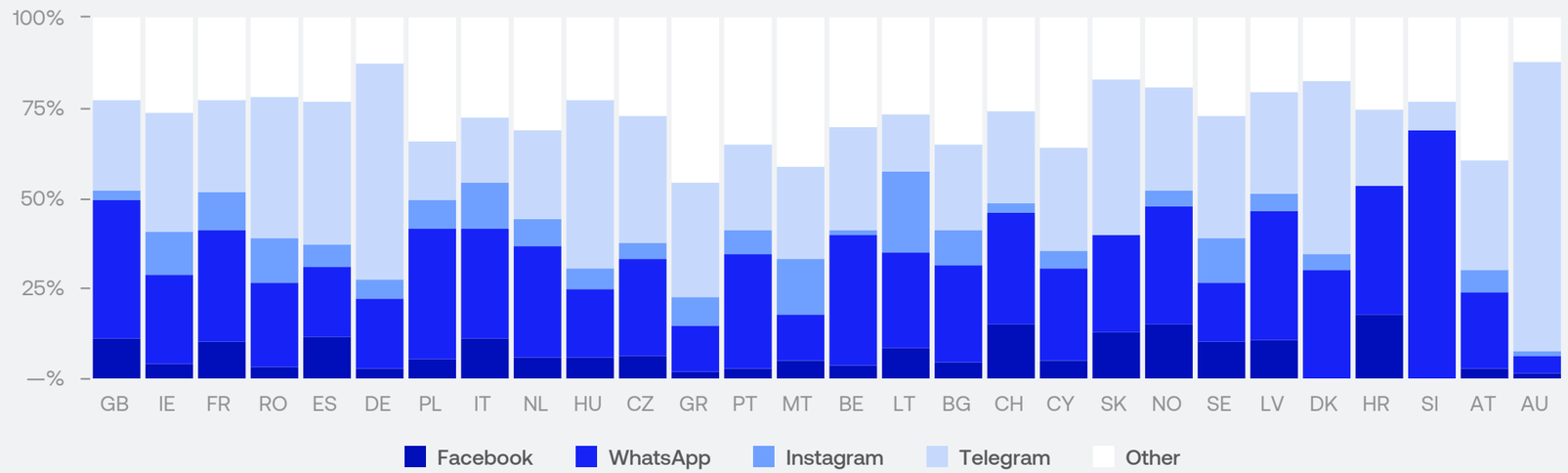
WhatsApp's Significant Role

WhatsApp also plays a significant role in facilitating investment scams, particularly in countries including Slovenia (69%), Belgium (36%), Latvia (36%), Croatia (36%), Switzerland (31%), France (31%), and Denmark (30%). This underscores how widely used messaging platforms are exploited for financial fraud, even those with encrypted services.

Other Platforms

While Telegram and WhatsApp are prominent, other platforms also contribute to investment scams. It's important to note the presence of "Other" as a significant category in several countries, indicating that investment scams occur across a range of platforms, such as Snapchat and TikTok.

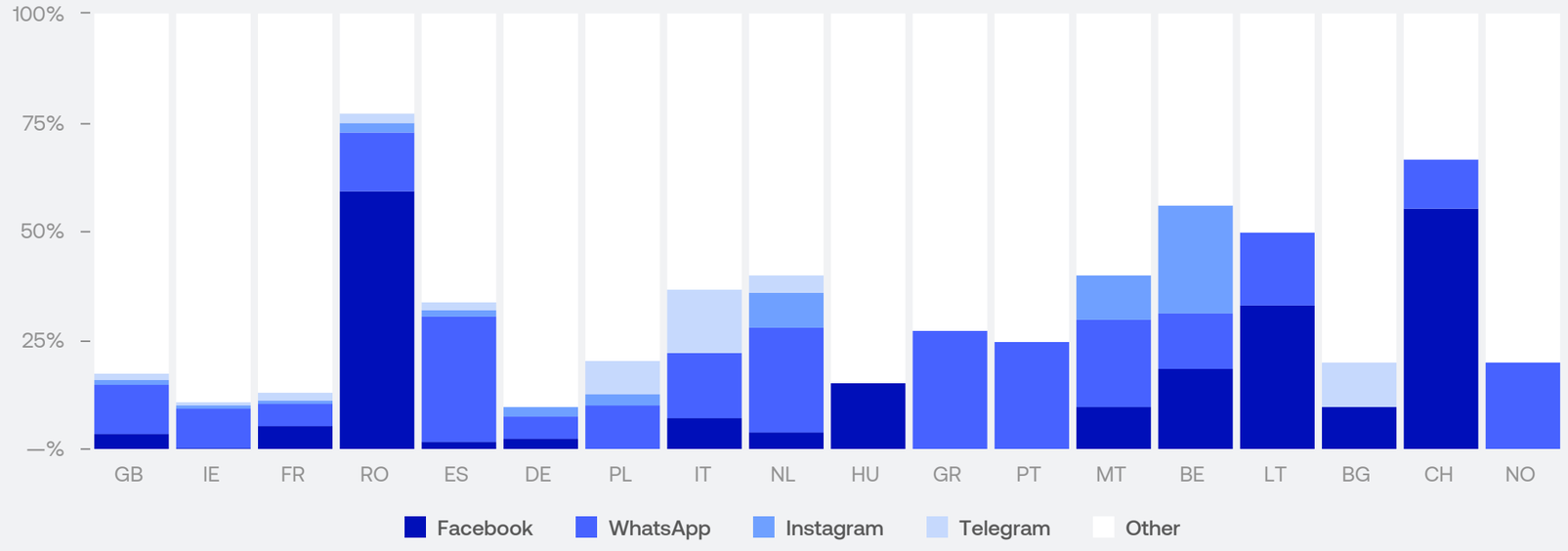
Exhibit 10 - Investment scam breakdown by source of Fraud



Impersonations scams

Impersonation scams utilise a wider range of platforms compared to other fraud types. However, Meta platforms (WhatsApp, Instagram, and Facebook) account for a significant percentage of reported cases in several countries, including Romania, Spain and Belgium.

Exhibit 11 - Impersonation scam breakdown by source of Fraud



How to identify a scam

Revolut continues to educate customers on the different types of fraud by providing valuable information that helps them remain vigilant.

Understanding how to detect various types of scams and fraud is crucial for consumers, especially given the alarming rise in fraudulent activities originating from social media platforms.

Recent data indicates a significant percentage increase in scams 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:

- Inconsistent stories. If what they say doesn't add up, or changes frequently, customers need to be wary.
- 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.

Exhibit 12 - Revolut educational content on job scams

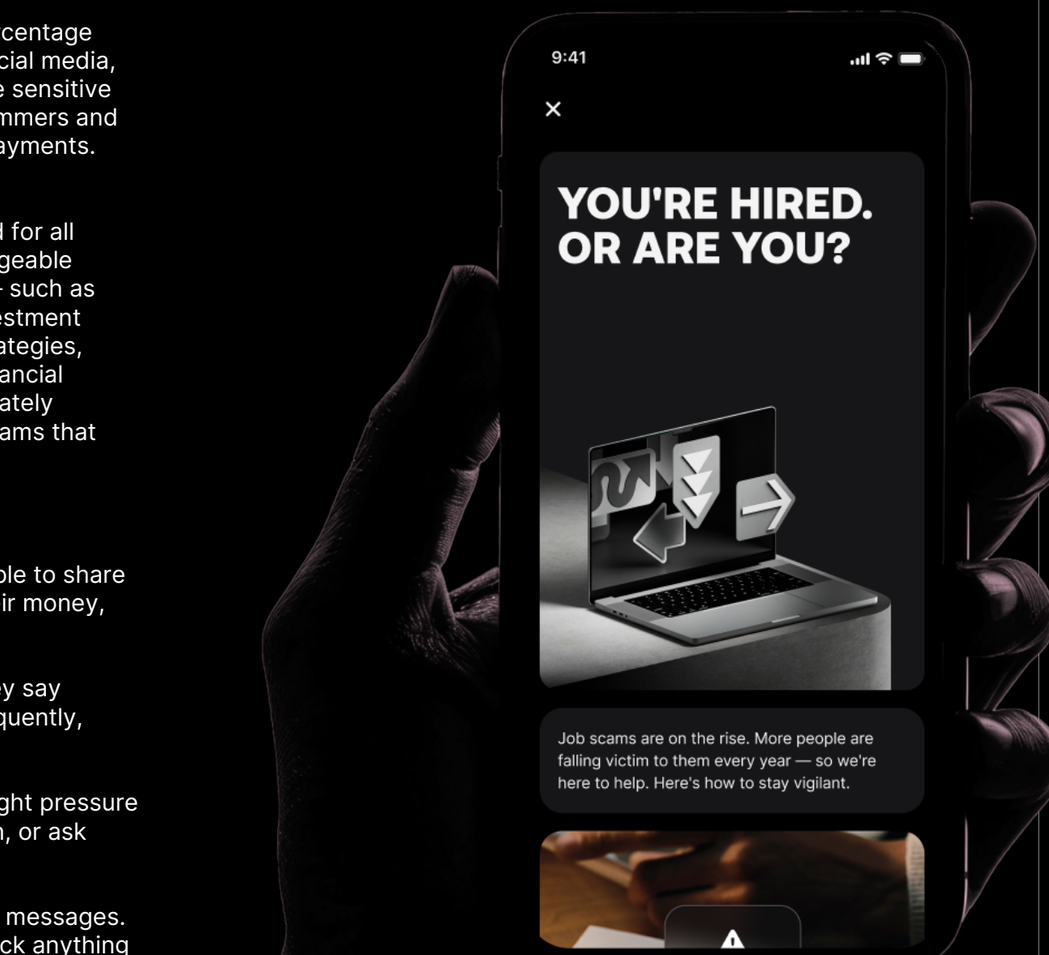


Exhibit 13 - Revolut educational content on purchase scams

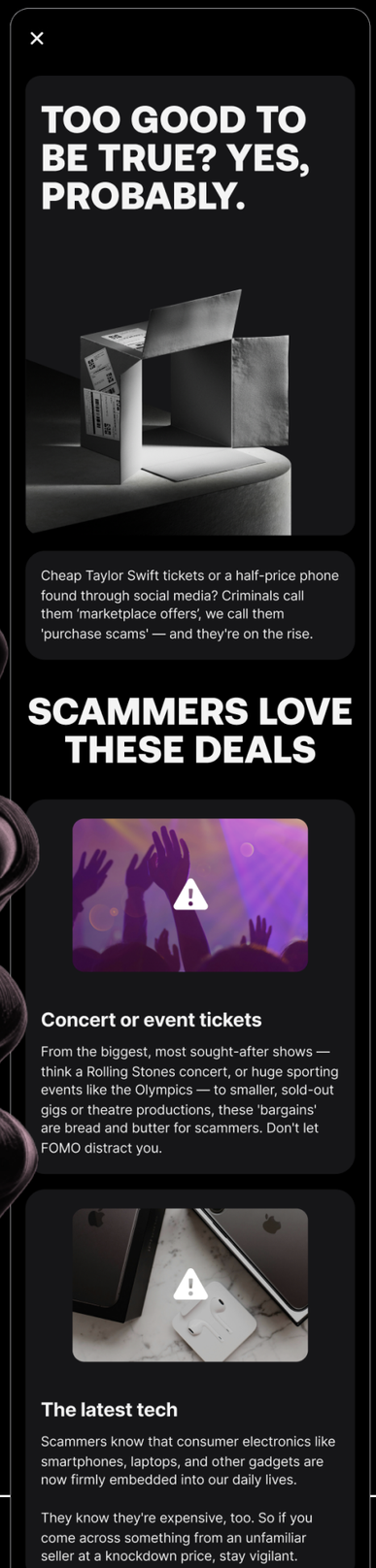
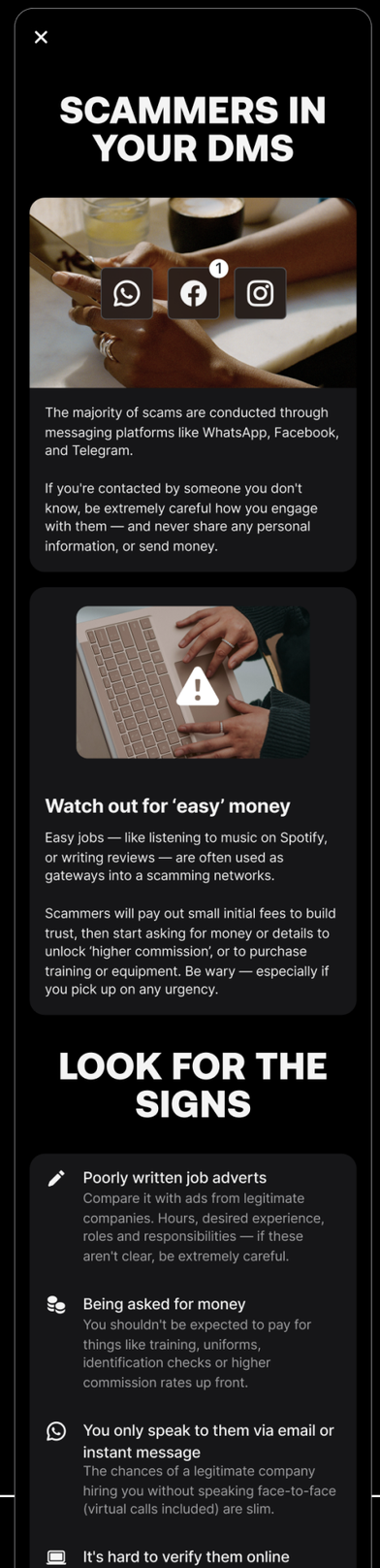
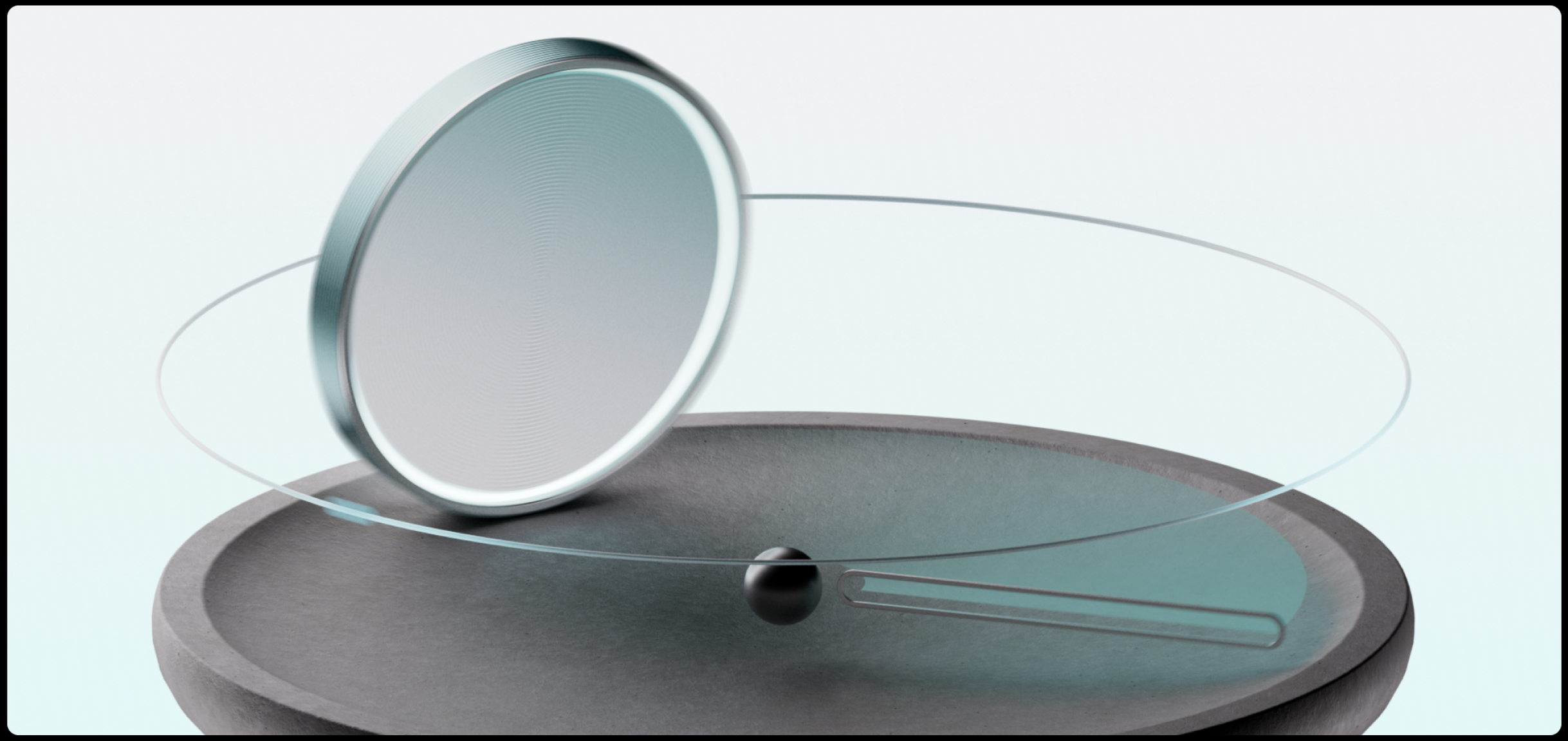


Exhibit 14 - Revolut educational content on investment scams



Unauthorised fraud deep dive: global overview



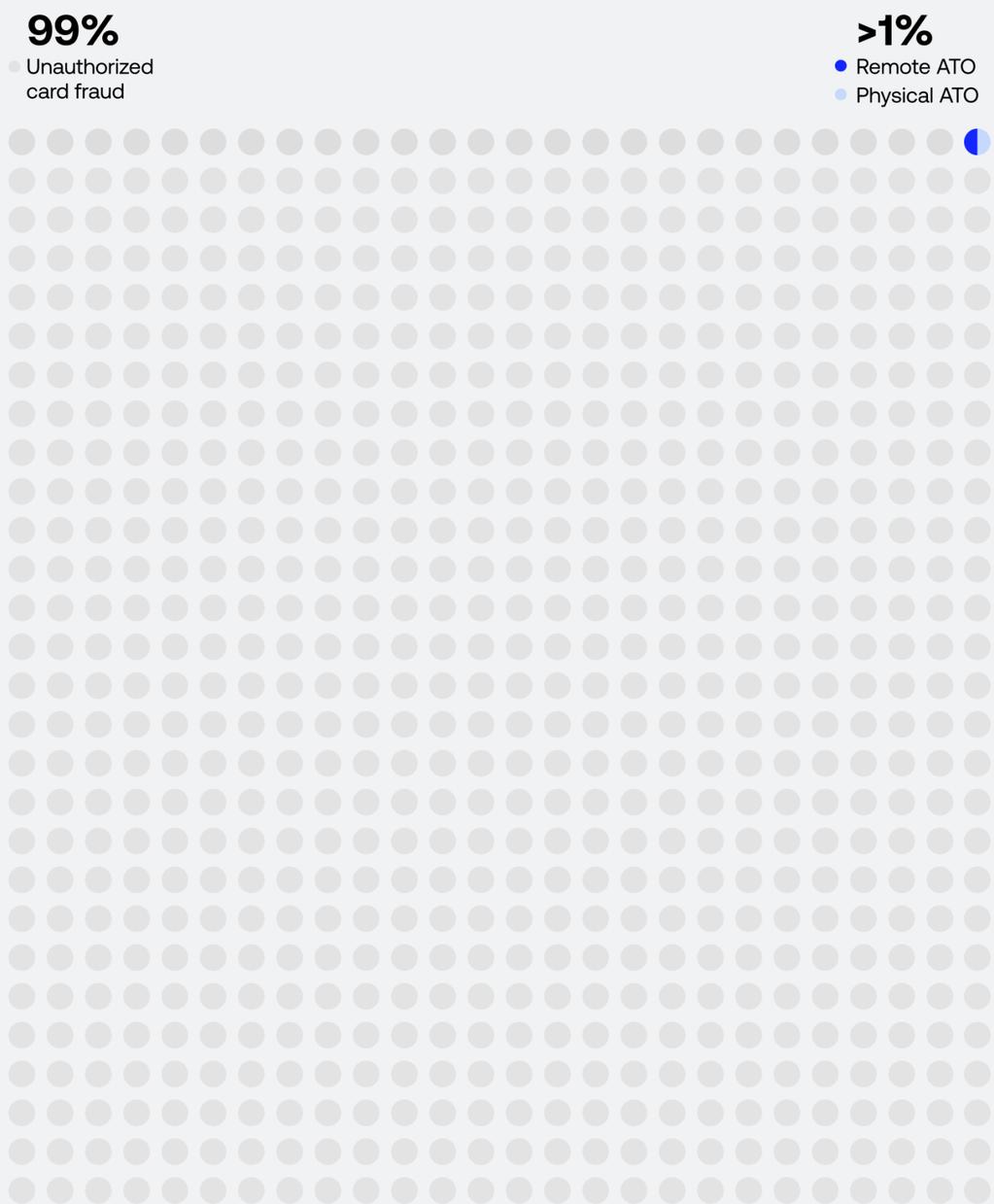
Building upon our understanding of scammer tactics, and the knowledge that they operate mostly on social media, it's equally crucial to delve into the mechanisms behind unauthorized fraud. This occurs when criminals illicitly obtain personal information, allowing them to compromise accounts and initiate unauthorized transactions.

The data clearly indicates that unauthorized card fraud remains the dominant form of attack, consistently accounting for nearly 100% of reported cases over the 18 months from July 2023 to December 2024.

However, while the prevalence of card fraud persists, it's noteworthy that preventative measures, such as disposable virtual cards for single-use transactions, implemented by Revolut and the wider financial sector, have played a significant role in mitigating the impact of these attacks.

Furthermore, the chart 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 and advanced fraud detection systems, are effectively minimizing these types of unauthorized access.

● Exhibit 15 - Unauthorised Fraud breakdown by type of fraud H2'24



How Revolut is fighting fraud

At the forefront of Revolut's security measures is its proprietary fraud detection system, employing cutting-edge machine learning and artificial intelligence methodologies.

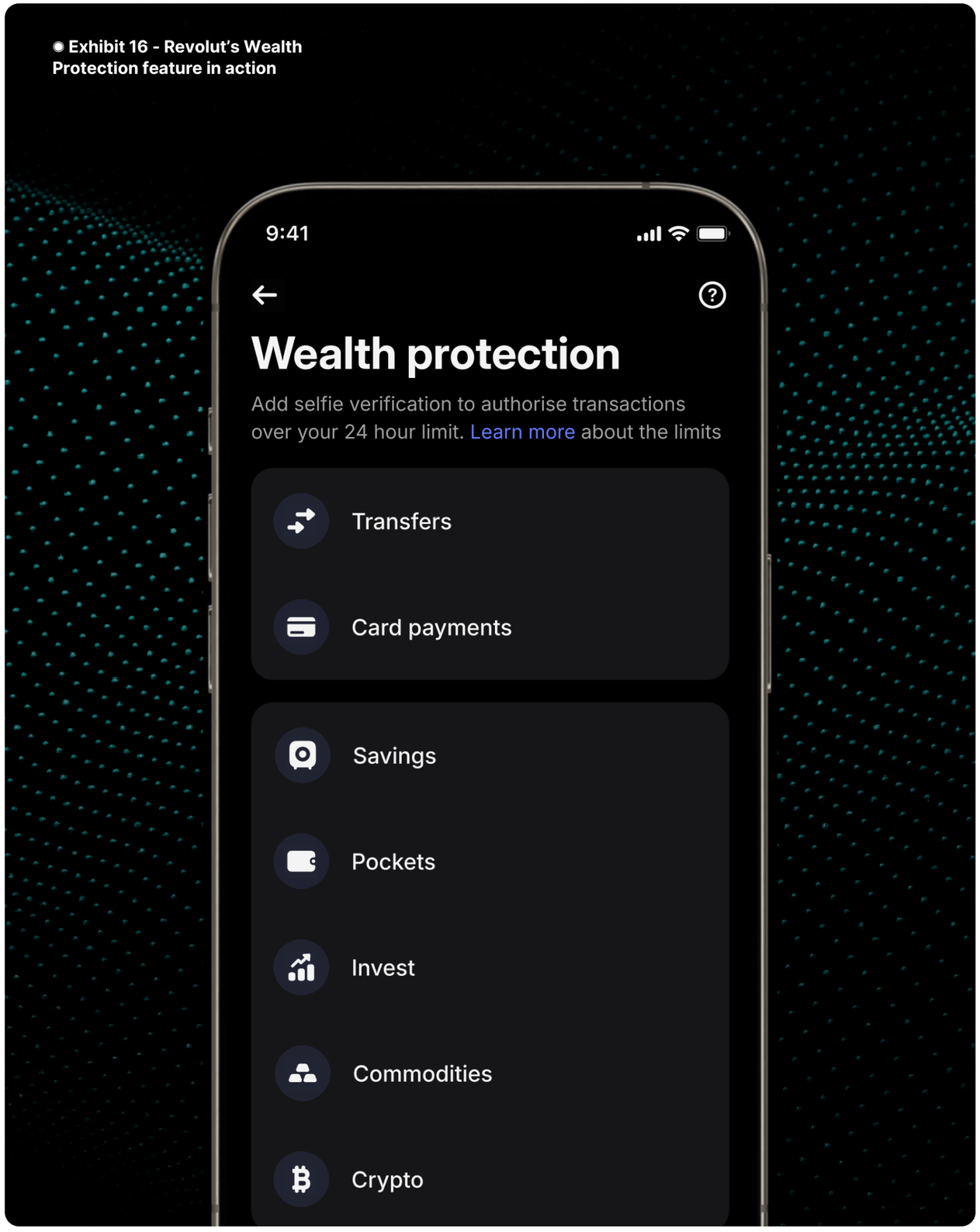
Revolut estimates that in 2024, it prevented over £600 million in fraud against its customers.

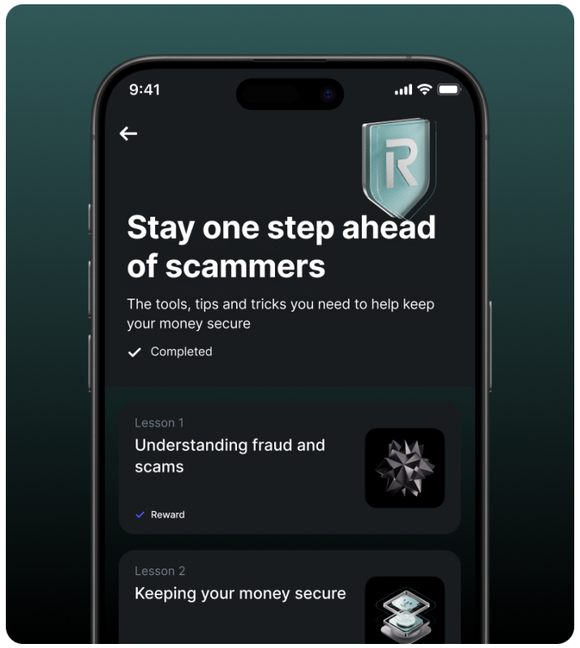
Staying ahead of the dynamic fraud landscape, Revolut continually monitors its evolution and responds swiftly by implementing enhanced customer security features.

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, Personal Pockets, and crypto trades and transfers.

Exhibit 16 - Revolut's Wealth Protection feature in action

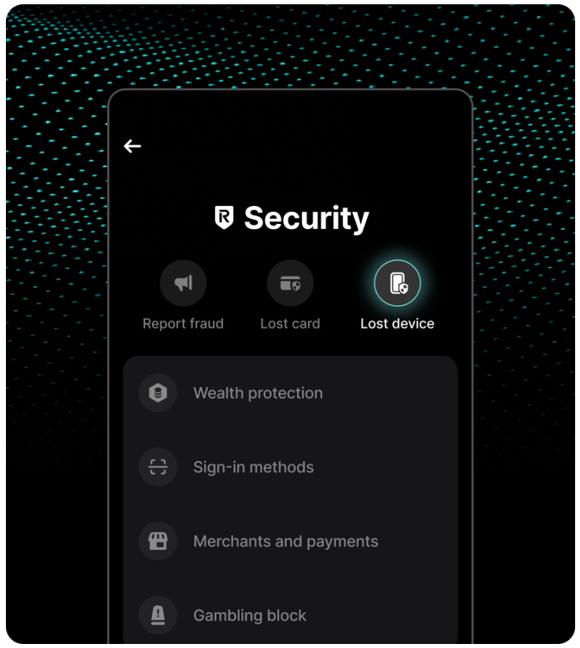




Fraud Learn 2.0

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

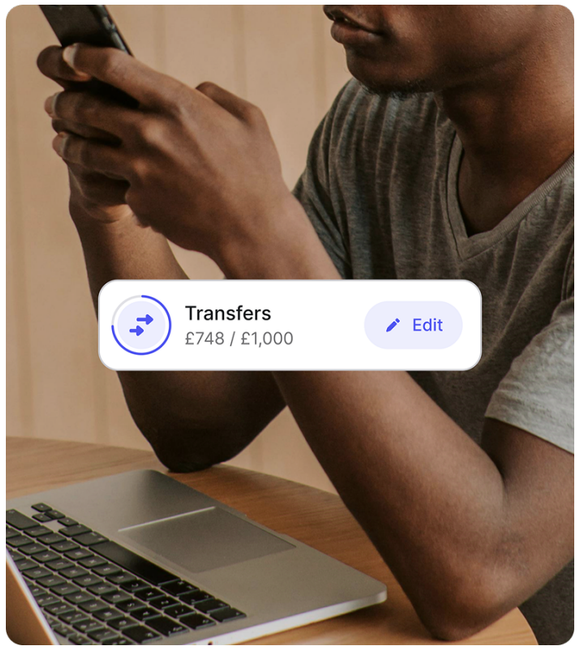
Customers can learn about the common trends in fraud and scams, and learn to recognise the warning signs of risky transactions and bad actors.



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.



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.

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.

Conclusions

The data presented in this report paints a stark picture. While sophisticated scams targeting consumers take various forms, from purchase and job schemes to intricate investment frauds, the common thread weaving through these illicit activities is their pervasive presence on social media platforms, especially those under the Meta umbrella.

Despite ongoing efforts, the reality is that social media platforms are failing to adequately address the rampant fraud plaguing their users. The fact that over 55% of reported authorized fraud cases originate from Meta platforms, with Facebook alone accounting for over a third, underscores the inadequacy of current preventative measures. These figures are not just statistics; they represent real people, real losses, and a significant breach of trust.

At Revolut, we remain steadfast in our commitment to safeguarding our customers through advanced security features, enhanced protections, and a dedicated team of financial crime experts. However, it's abundantly clear that financial institutions cannot shoulder this burden alone. We cannot be the sole line of defence against a threat that is incubated and disseminated on social media platforms.

The time for incremental improvements is over. Social media platforms must fundamentally transform their approach to fraud prevention. This necessitates more than just reactive measures; it demands proactive intervention, including the implementation of robust AI-driven monitoring, stringent verification processes for advertisers and content creators, and seamless collaboration with financial institutions and law enforcement.

Until social media platforms, particularly Meta, demonstrate a genuine commitment to eradicating fraud from their ecosystems, consumers will remain dangerously exposed. We urge governments and regulatory bodies to hold these platforms accountable and mandate the implementation of effective anti-fraud measures.

As we move forward, Revolut will continue to empower our customers with the knowledge and tools they need to protect themselves. However, true progress hinges on a collective effort – one where social media platforms finally acknowledge their responsibility and take decisive action to help us and other financial institutions create a safer digital environment for all.

Revolut Group Holdings Ltd
Registered number: 12743269