Revolut

Consumer Security and Financial Crime Report H1’24

Revolut Group Holdings Ltd
Registered number: 12743269

CONTENTS

04
What is fraud?

16
How to identify a scam

22
Conclusions

Woody Malouf, Head of Financial Crime at Revolut, on the second edition of our Consumer Security and Financial Crime Report H1'24

Fraud is a global problem, impacting people and businesses worldwide. Financial criminals continue to intensify their efforts, employing sophisticated tactics such as deceptive websites, elongated payment chains, and social engineering attacks to ensnare victims. In 2023, global citizens lost over USD $1 trillion to fraud, with 78% of people experiencing at least one scam attempt in 2023, according to GASA (Global Anti-Scam Alliance & ScamAdviser, Global State of Scams report).

Our ultimate goal is to enhance the protection of everyday people and increase awareness. It is the reason we invest heavily in the safety and security of our customers, helping to protect them against new and existing types of fraud and scams.

We understand how fraud and scams can affect our customer's daily lives. Our goal is to use effective fraud prevention measures to protect them and ensure good outcomes.

Further, in the fight against fraud, we need up-to-date intelligence to help better understand and address the key drivers.Today, six months on from our inaugural report, we are publishing the second edition of our Consumer Security and Financial Crime Report. 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

This edition also includes:

- a breakdown of where each type of fraud most frequently originates
- a deep dive on ticket scams, following increasing volumes over the last six months (driven by seasonal events over the summer months)

Our 4,000-strong, 24/7 financial crime team employs advanced AI-based algorithms, alongside biometric tools and cybersecurity measures. This meant over £475m of potential fraud against our customers was prevented in 2023 alone — and already more than £250m in H1 2024.

To counter the ever-changing tactics of fraudsters, Revolut is constantly strengthening its set of tools and techniques to prevent, detect, and disrupt fraudulent activity. The technology used by fraudsters to trick innocent people is increasingly sophisticated, and therefore our systems need to be even more so.

There's an 'arms race' taking place between financial institutions and fraudsters, and to win, we need to constantly evolve. We're as committed as ever to protecting our customers from today's fraudsters — and tomorrow's, too.

There's no single solution or institution that can tackle this issue alone. While financial institutions play a crucial role, this is a broader problem that spans the entire ecosystem. It requires coordinated efforts from governments, social media platforms, regulators, and financial institutions alike. Only by working together can we effectively combat these ruthless criminals and safeguard our systems. Everyone—whether in finance, government, or tech—must step up and do their part.

Methodology

The findings in this report are based on anonymised data from the Revolut platform, spanning an 18-month period between 1 January 2023 - 30 June 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:

1 — **Unauthorised Fraud** (or "Fraud") and Authorised Fraud (or "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.

2 — **Authorised Fraud**, or "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:

1 — **Physical Theft** - This is when fraudsters steal the device or phone itself and are able to make payments or transfer out funds.

2 — **Account Takeover (ATO)** - This is when fraudsters are able to take control of someone's account to make payments or transfer out funds. This can be done remotely by gaining access to the customer's password and account information or by hacking into the phone.

3 — **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 might not be 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:

1 — **Purchase Scams:** Scammers often use social media marketplaces like Facebook Marketplace to lure victims by offering unbelievably low prices on products that are never delivered. Another common scam involves fraudulent rental listings, where scammers post fake rental properties and request upfront deposits from unsuspecting renters.

2 — **Investment Scams**: Fraudsters convince users to transfer funds or cryptocurrencies by offering fake investment opportunities with lucrative returns. Investment news articles or social media posts endorsed by celebrities that highlight opportunities to make high returns on their money through crypto investments are a common scam tactic.

3 — **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 ask people to pay upfront for paid training, administration, and setup fees, or to purchase required equipment, such as a laptop or phone.

4 — **Impersonation Scams**: Scammers pretend to be bank officials, government agents, or even bank agents contacting you about unpaid fees or loans. They might sound serious, asking for immediate payments or personal details to fix supposed issues.

5 — **Relationship/Romance Scams**: Scammers create a new romantic connection with the victim, building up trust over the course of weeks or months. Fraudsters will then ask for some money using an emergency or travel plans as an excuse and then disappear.

6 — **Invoice Scams**: Also known as mandate fraud, is when fraudsters pose as a subscription service, merchant, or service provider, and tell you that 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.

7 — **Tax Scams:** Scammers pretend to be tax officials or cops, making urgent calls about unpaid taxes. They might even imply that you will be arrested soon if you do not make the payment urgently.

8 — **Loan Scam:** 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.

Other types of fraud

Triangle Scams[1] are a combination of two or more types of scam, used by fraudsters to avoid detection. In triangle scams, there are two victims; Victim A is defrauded into making a payment to Victim B's account, and Victim B is subsequently defrauded into making a second likely bigger payment to the fraudster's account. This chain of payments makes it difficult for the authorities to identify and trace the fraudster.

Here's an example of how a triangle scam combining two investment scams may operate:

Fraudster
Hey, can I buy your crypto for **$500**?

You
Sure, here are my bank details

Fraudster on P2P exchange wants your crypto, says their friend will pay you.

Fraudster
Wanna earn $2,000?

You
Yes, but how?

Fraudster
Through high return investments! Just send **$500** to this account, and get 4x more in a few days

You
Sure thing, sending now!

Behind the scenes, the fraudster tricks another victim, directing them to send money to your account.

Second victim
- $500

First victim
+ $500
-$500 in crypto

Fraudster
+$500 in crypto

You receive the promised money and send the fraudster your crypto.

[1] Learn more about P2P crypto scams here

GLOBAL FRAUD AND SCAMS TRENDS

Prevalence and impact of authorised vs. unauthorised fraud

Since January 2024, we've seen an increase in consumers falling victim to authorised fraud. Last year, in the UK alone, the volume of authorised push payment (APP) fraud cases increased by 12% YoY from 2022, resulting in a total loss of £459.7million [UK Finance, 2024].

This type of fraud, often referred to as a 'scam', involves sophisticated social engineering tactics, where fraudsters manipulate individuals into authorising payments or transferring money from their accounts.

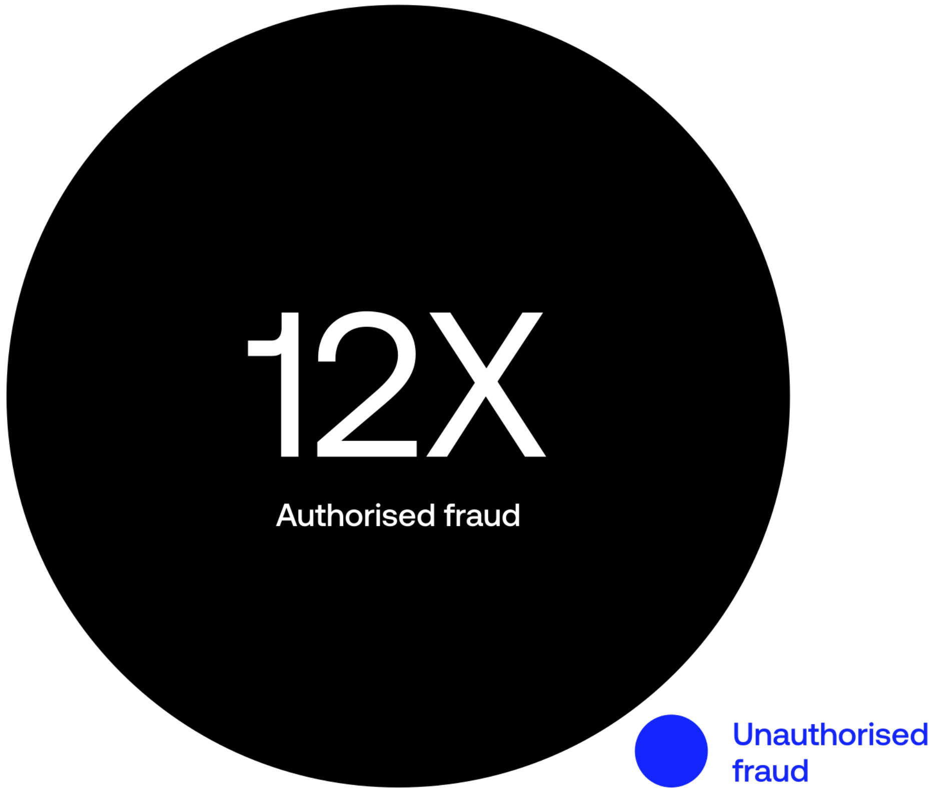
Common methods that criminals employ include impersonating trusted entities — such as financial institutions, government agencies, or service providers — often through phone calls, emails, or social media.More details can be found in the Impersonation Scam section on page 15.

Authorised fraud has become a significant vulnerability for consumers, accounting for nearly 50% of total fraud cases by the end of H1 2024, as shown in Exhibit #1. This shift suggests that fraudsters are increasingly targeting authorised fraud as authentication becomes more secure, with the average financial loss from an authorised fraud case being over 12 times greater than that from unauthorised fraud.

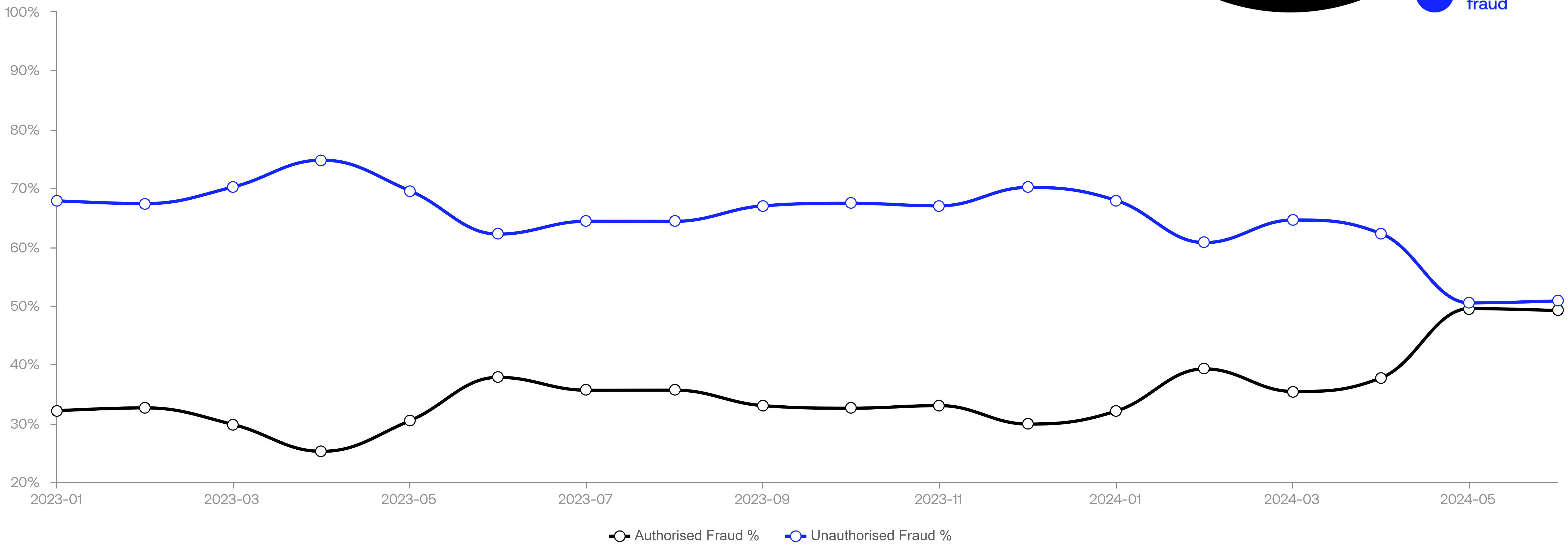
Financial institutions, such as Revolut, play a critical role in protecting consumers by issuing warnings and alerts when potential scams are detected.

In the next chapter, we'll explore the operational mechanics of authorised fraud — digging into the most common types of scams, and examine the key sources behind the rise of these fraudulent activities.

◉ Exhibit #2 - Authorised Fraud vs. Unauthorised Fraud: average loss per victim H1'24



◉ Exhibit #1 - Authorised Fraud vs. Unauthorised Fraud: distribution of victims (2023 - H1'24)



AUTHORISED FRAUD DEEP DIVE GLOBAL OVERVIEW

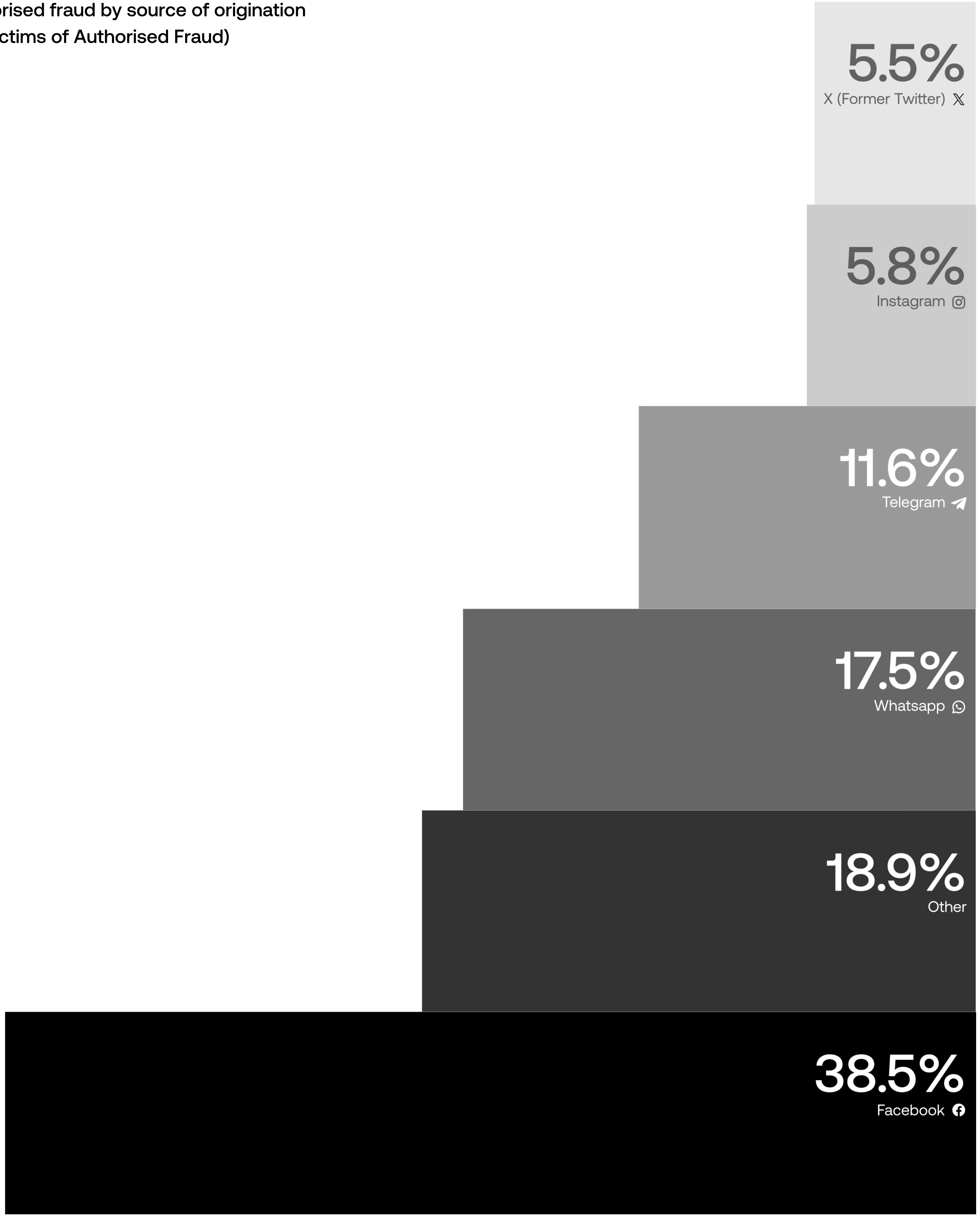
Where does Authorised Fraud most commonly originate?

+60%

of all authorised fraud victims originated on Meta platforms (Facebook, WhatsApp, and Instagram) during the first half of 2024.

Facebook accounts for the highest percentage of authorized fraud victims, representing 38.5% of the total, followed by WhatsApp at 17.5% and Telegram at 11.6% In terms of total losses, Meta platforms collectively account for over 50% of the total Authorised Fraud amount lost.

◉ Exhibit 3 - Authorised fraud by source of origination H1'24 (% of total victims of Authorised Fraud)



Which APP scams are most prevalent?

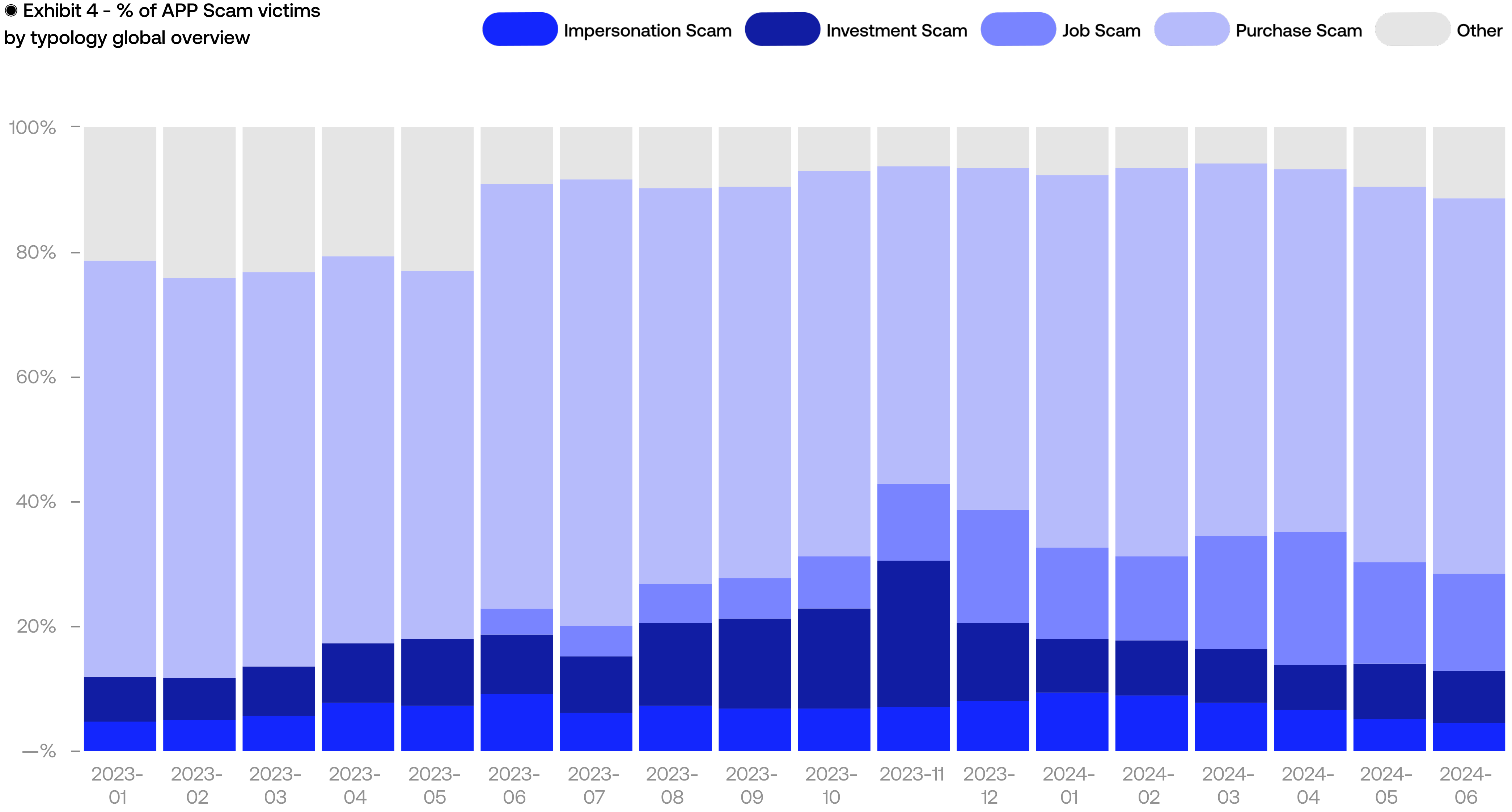
A deeper examination of the most common forms of authorised fraud reveals some notable shifts.

Since April 2024, there has been a surge in fraudsters targeting consumers through job scams. These scams target individuals searching for employment, or employed individuals looking to make extra income due to cost of living challenges. These individuals are exploited through the offer of what seem like promising job opportunities — requiring individuals to complete tasks, often linked with performing investments and crypto trading, using their own money. This money, in most cases, then disappears.

By the end of 2023, job scams accounted for less than 9% of all reported authorised push payment (APP) scams. However, by the end of June 2024, their share had almost doubled — indicating a sharp rise in prevalence.

Despite this increase, purchase scams remain the most prevalent type of scam, accounting for over 60% of total scam victims. This has remained consistent over the past year, as purchase scams continue to be the most common tactic used by fraudsters to deceive victims. The prevalence of specific fraud types varies across countries (as shown in Exhibit 5), indicating that certain tactics are either more commonly employed, or that customers are more susceptible to different scam types based on their geographic location.

● Exhibit 4 - % of APP Scam victims by typology global overview



Top 3 types of APP Scams

+60%

of APP cases were **Purchase Scams in H1'2024**

17%

of APP cases were **Job Scams in H1'2024**

8%

of APP cases were **Investment Scams in H1'2024**

From the country breakdown, we can identify a number of key takeaways:

Country cluster for job scams:

In Spain (ES), Italy (IT), Greece (GR), Portugal (PT), and Bulgaria (BG), the percentage of job scams is significantly higher than the global average (at least 20 percentage points above). This disparity may be attributed to factors such as higher unemployment rates or more competitive job markets in these regions — fertile grounds for fraudsters to exploit vulnerable job seekers via messaging apps or social media.

Prevalence of purchase scams:

In all markets except Italy, purchase scams are the most common type of APP fraud. This indicates they're the dominant fraud type across most countries — highlighting universal vulnerabilities, as well as the global reach of online marketplaces and social media platforms.

Impersonation scams and other types:

Impersonation scams are more prevalent in Finland (FI), Great Britain (GB), and Ireland (IE) compared to other countries. Fraudsters take advantage of a psychological factor known as 'compliance pressure,' where individuals feel rushed or emotionally manipulated — leading them to act without thoroughly verifying the legitimacy of a request.

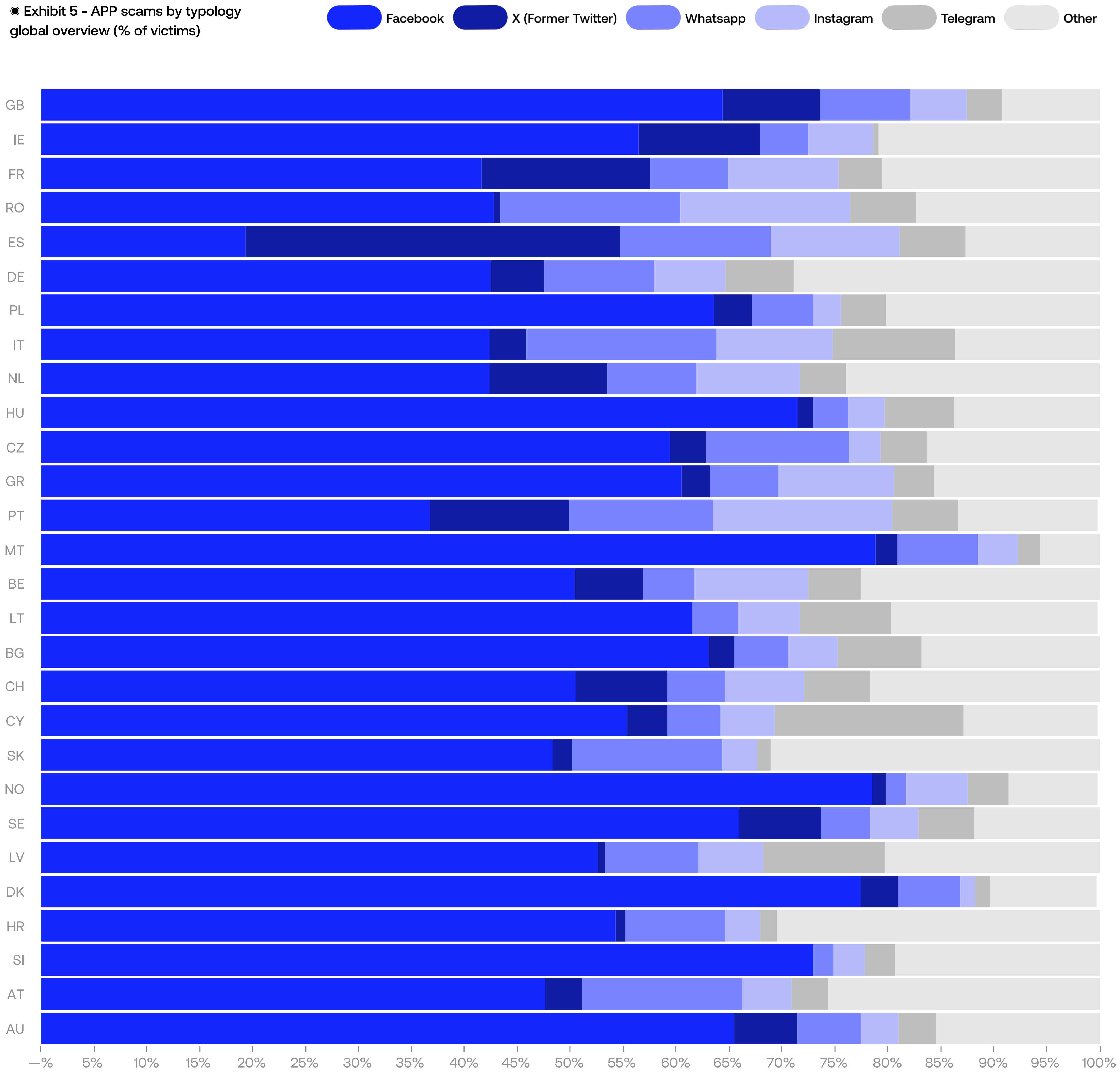
Investment scams:

Germany, Italy, Poland, Austria and Belgium have a greater share of investment scams. Promising high returns and minimal risk, fraudsters are frequently exploiting both inexperienced investors, and those eager for quick financial gains.

With the ability to recognise different patterns of fraud types by region or country, it's even more important to understand where these scams originate, and how they're executed.

Identifying the preferred channels scammers use to deceive consumers is critical in the fight against fraudsters. As highlighted in Exhibit 2, authorised fraud, on average, results in losses 10 times greater than unauthorised fraud.

● Exhibit 5 - APP scams by typology global overview (% of victims)



Revolut remains at the forefront of educating the public on fraud prevention, offering guidance on how to recognise potential scams.

The sections below provide valuable data and insights to support the ongoing fight against fraud, helping the public stay informed and vigilant by understanding new emergent trends in fraudster behaviours.

Purchase scams

As the most prevalent type of Authorised Push Payment (APP) fraud across most countries, this section looks more closely at purchase scams.

Facebook's global reach and the popularity of secondhand shopping on platforms like Facebook Marketplace have created an environment where fraudsters can easily exploit the trust and convenience of online shopping, allowing scams to flourish.

As shown in the graphic on the right side of the page (Exhibit 8), Facebook is the preferred platform for scammers to commit purchase scams across all markets. In many countries, including Great Britain (GB), Ireland (IE), Austria (AT), and Slovenia (SI), more than 75% of reported Purchase Scams originate on Facebook.

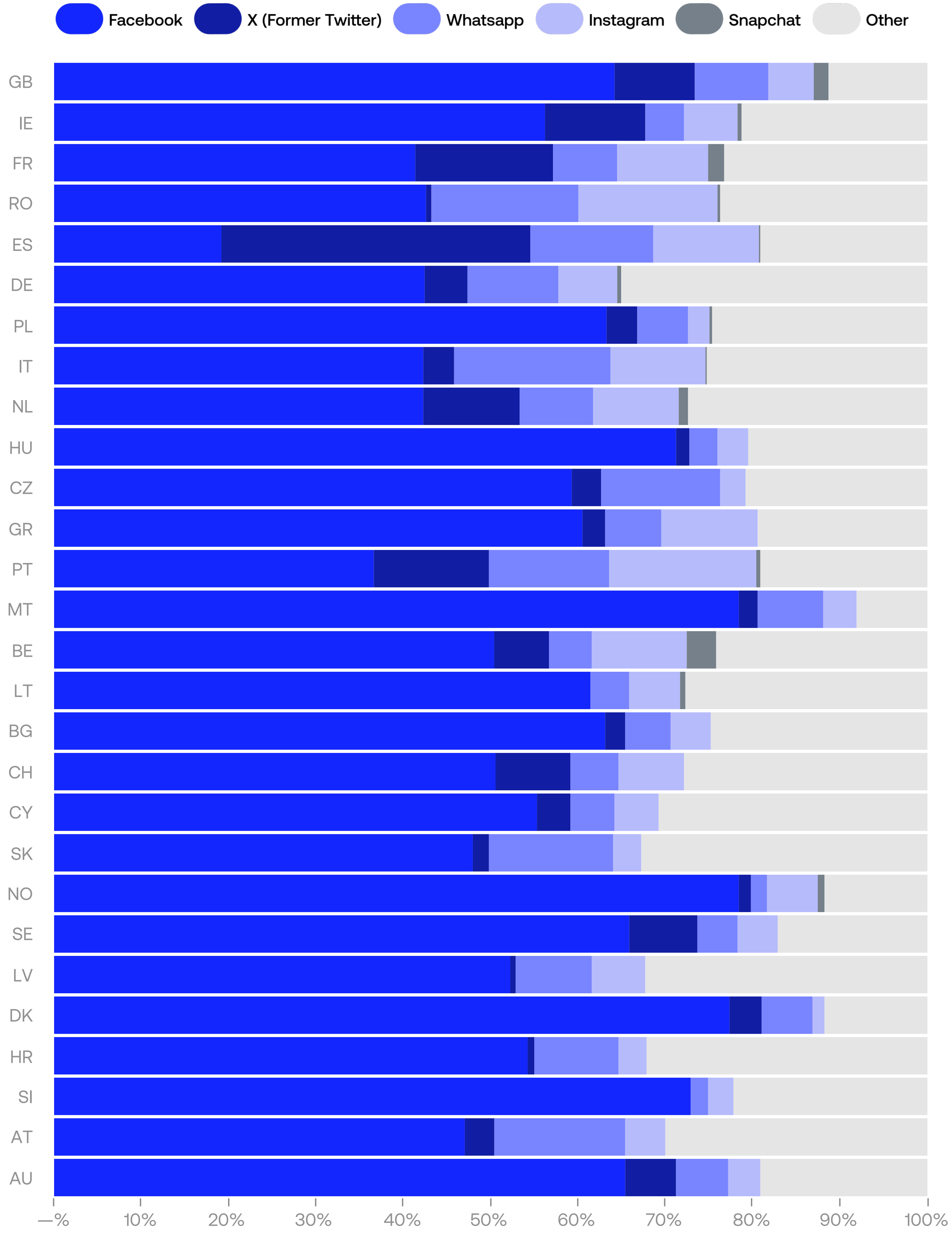
In countries like Poland (PL) and Germany (DE), a significant portion of scams also originate from other platforms like WhatsApp and Instagram, indicating a more diverse range of platforms used for scams.

Scammers in these regions are likely adapting to the communication habits of their targets, taking advantage of the widespread use of messaging apps and alternative social media for personal and business interactions. Encrypted messaging capabilities, including those leveraged by WhatsApp and Telegram, provide a sense of privacy and consumer trust that fraudsters exploit.

In Romania (RO), Italy (IT), Greece (GR) and France (FR) there's a higher use of Instagram and WhatsApp for purchase scams, compared to other countries.

Spain presents a particularly interesting deviation from the mean. Unlike the global trend, Spain is the only country in the data set where Facebook is not the predominant platform for purchase scams. Instead, X is the leading source of this type of authorised fraud — hosting more than 35% of purchase scams. Alongside Spain, Ireland (IE) and France (FR) also show a notable, though smaller, share of purchase scams originating from X.

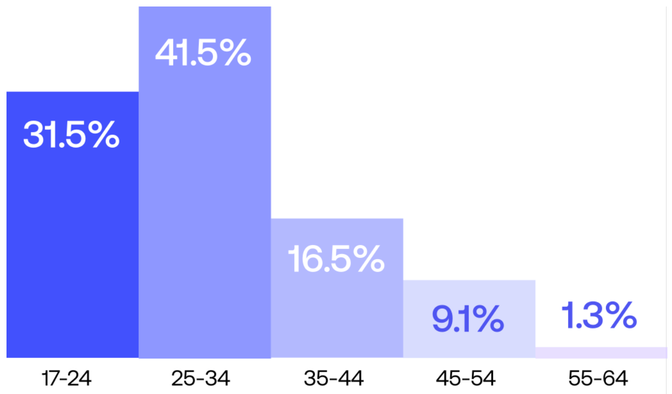
● Exhibit 6 - Purchase scam breakdown by source of Fraud - H1'24



Deep dive: Ticket scams

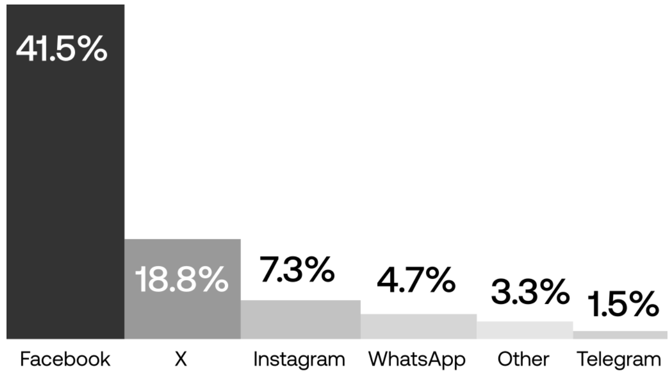
The first half of 2024 was defined by major global events like the Summer Olympics, Taylor Swift's record-breaking Eras Tour, and the European Championships.
While these events united millions of fans, they also provided fertile ground for scammers to prey on individuals eager to secure tickets.

● Exhibit 7 - % of Victims of Ticket scams per age group (June'24)



Looking specifically at June 2024, as the graphic above (Exhibit 7) shows, more than 70% of ticket scam victims were consumers between 17-34 years of age. These combined demographics appear to be particularly vulnerable to this type of fraud.

● Exhibit 8 -% of Victims of Ticket scams by platform (June'24)



Mirroring the pattern seen for general purchase scams, Facebook is where the majority of ticket scam victims are reported.

In June, over 40% of total ticket scams happened through Facebook alone. X followed with nearly 20% of reported cases, and WhatsApp, Instagram, and Telegram collectively accounted for just over 12% of reported ticket victims, showing that while these platforms are less dominant, they still present a notable risk for consumers.

Job scams

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

While Facebook is the predominant source of purchase scams, there's a higher concentration of job scams taking place on Whatsapp.

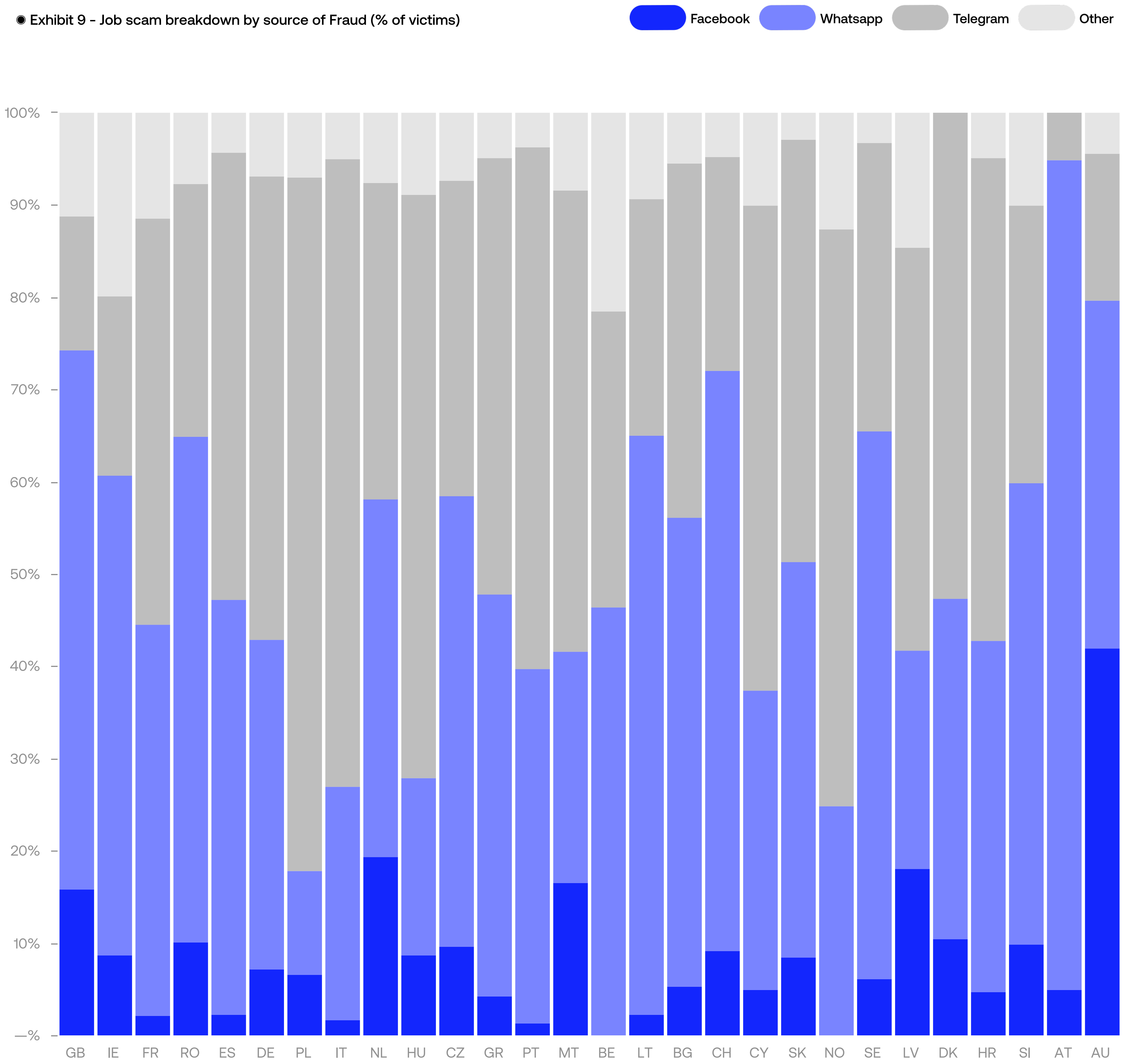
This shift in platform preference highlights the more targeted and conversational nature of job scams, where fraudsters use the perceived privacy and trust of these apps to deceive potential victims more effectively.

In countries including Great Britain (GB), Austria (AT), Norway (NO), Ireland (IE), Switzerland (CH), and Lithuania (LT), WhatsApp is the platform most commonly used by fraudsters to commit Job Scams.

Telegram seems to be the preferred platform for Job Scammers in Poland (PL), Italy (IT), Portugal (PT), Hungary (HU) and Cyprus (CY).

Australia (AU) stands out as the only market where Facebook and WhatsApp share an almost equal proportion of Job Scam activity, suggesting fraudsters in Australia 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 (% of victims)



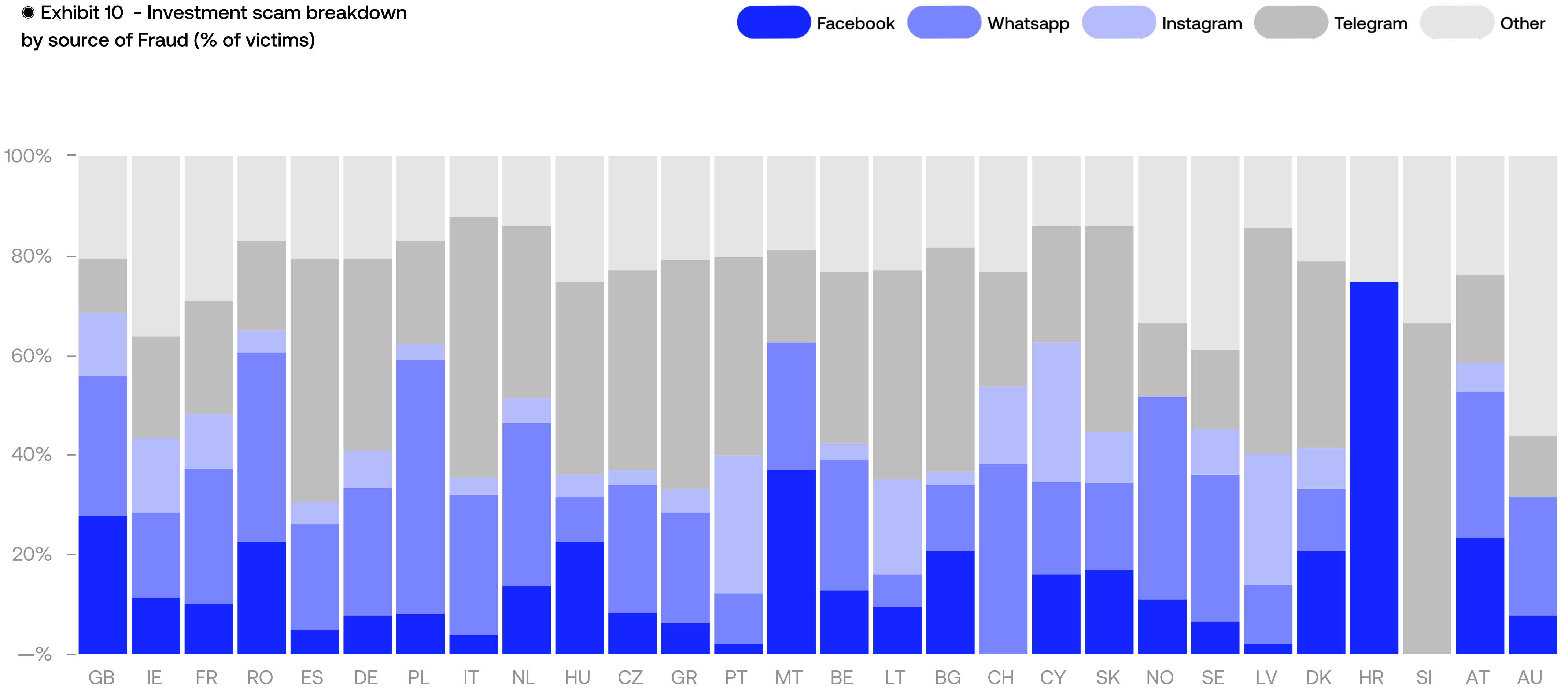
Investment scams

WhatsApp has also emerged as the predominant platform for investment scams in a number of countries.

In Norway (NO), Denmark (DK), Belgium (BE), Romania (RO), Austria (AT), and Great Britain, (GB), for example, 50% of reported investment scams took place on Whatsapp.

When looking at investment scam trends, Telegram poses a similar threat to consumers, particularly in countries such as Italy (IT), Spain (ES), Greece (GR), and Hungary (HU). Like WhatsApp, its encrypted messaging features and wide adoption make it an attractive tool for fraudsters to prey on victims looking for financial gain.

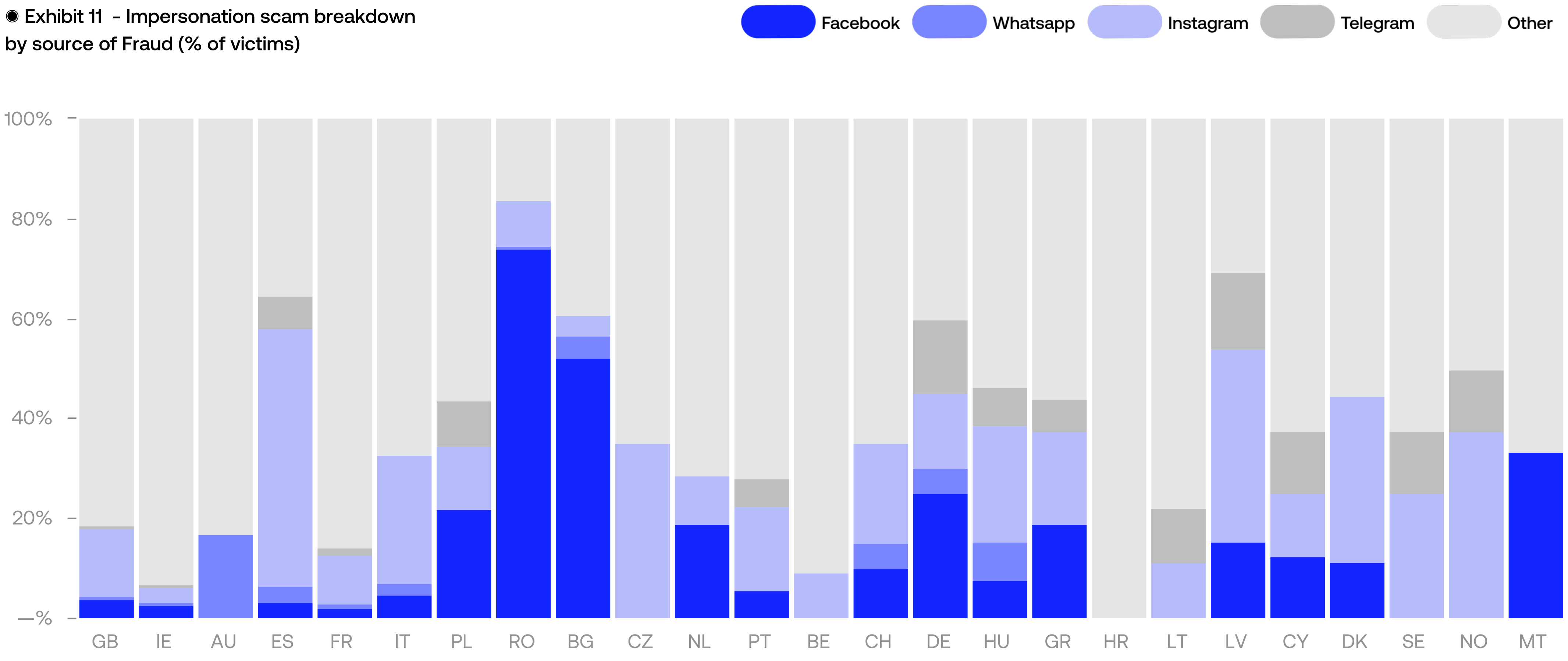
● Exhibit 10 - Investment scam breakdown by source of Fraud (% of victims)



Impersonations scams

When analysing the source of fraud data for impersonation scams by country, two key observations emerge. First, scammers use a more diverse range of platforms compared to other types of fraud. However, it's evident that in countries like Romania, Italy, and Spain, Meta platforms (WhatsApp, Instagram, and Facebook) account for a significant percentage of the reported cases.

● Exhibit 11 - Impersonation scam breakdown by source of Fraud (% of victims)



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.

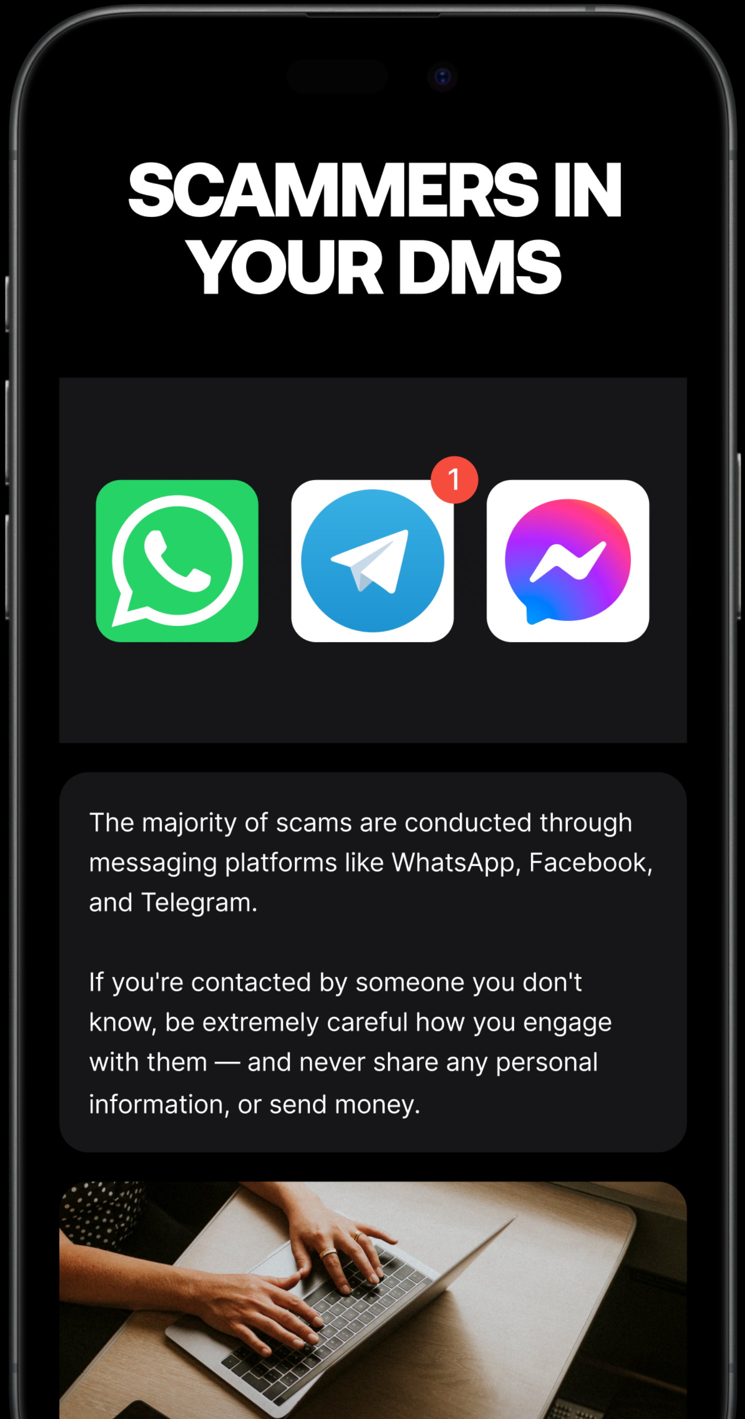
Recent data indicates a significant percentage increase in scams initiated through social media, where users, often unknowingly, share sensitive personal information directly with scammers and are socially engineered to authorise payments.

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 purchase scams

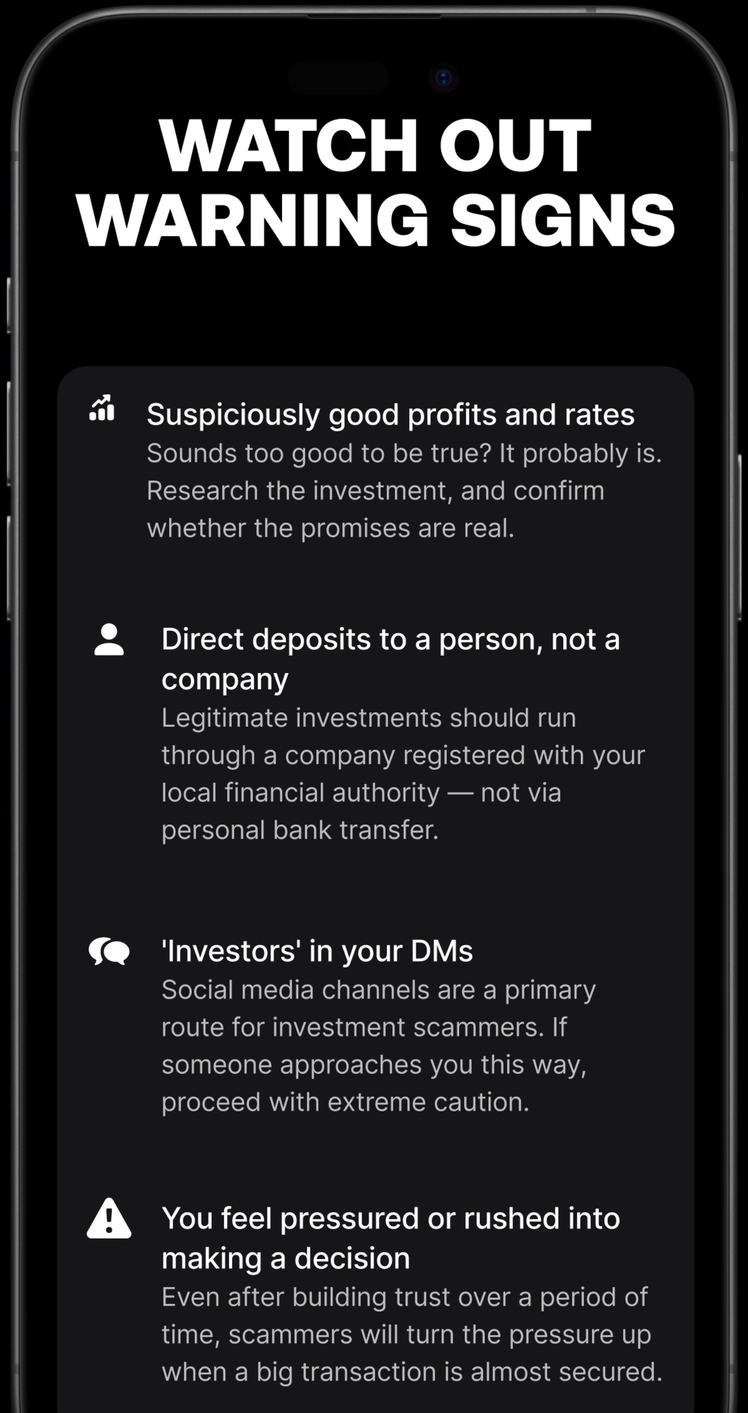


SCAMMERS IN YOUR DMS

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.

● Exhibit 13 - Revolut educational content on investment scams



WATCH OUT WARNING SIGNS

Suspiciously good profits and rates
Sounds too good to be true? It probably is. Research the investment, and confirm whether the promises are real.

Direct deposits to a person, not a company
Legitimate investments should run through a company registered with your local financial authority — not via personal bank transfer.

'Investors' in your DMs
Social media channels are a primary route for investment scammers. If someone approaches you this way, proceed with extreme caution.

You feel pressured or rushed into making a decision
Even after building trust over a period of time, scammers will turn the pressure up when a big transaction is almost secured.

UNAUTHORISED FRAUD GLOBAL OVERVIEW

Global overview

Now that we've examined how scammers operate (highlighting their varying tactics to deceive people into willingly transferring funds or making payments), and identified their preferred social media platforms across unique markets, it's important for consumers to also understand how unauthorised fraud occurs.

It happens when criminals gain unauthorised access to personal details, which may then be used to take over accounts, initiate unauthorised payments, or even apply for credit products including loans, retail finance, and credit cards.

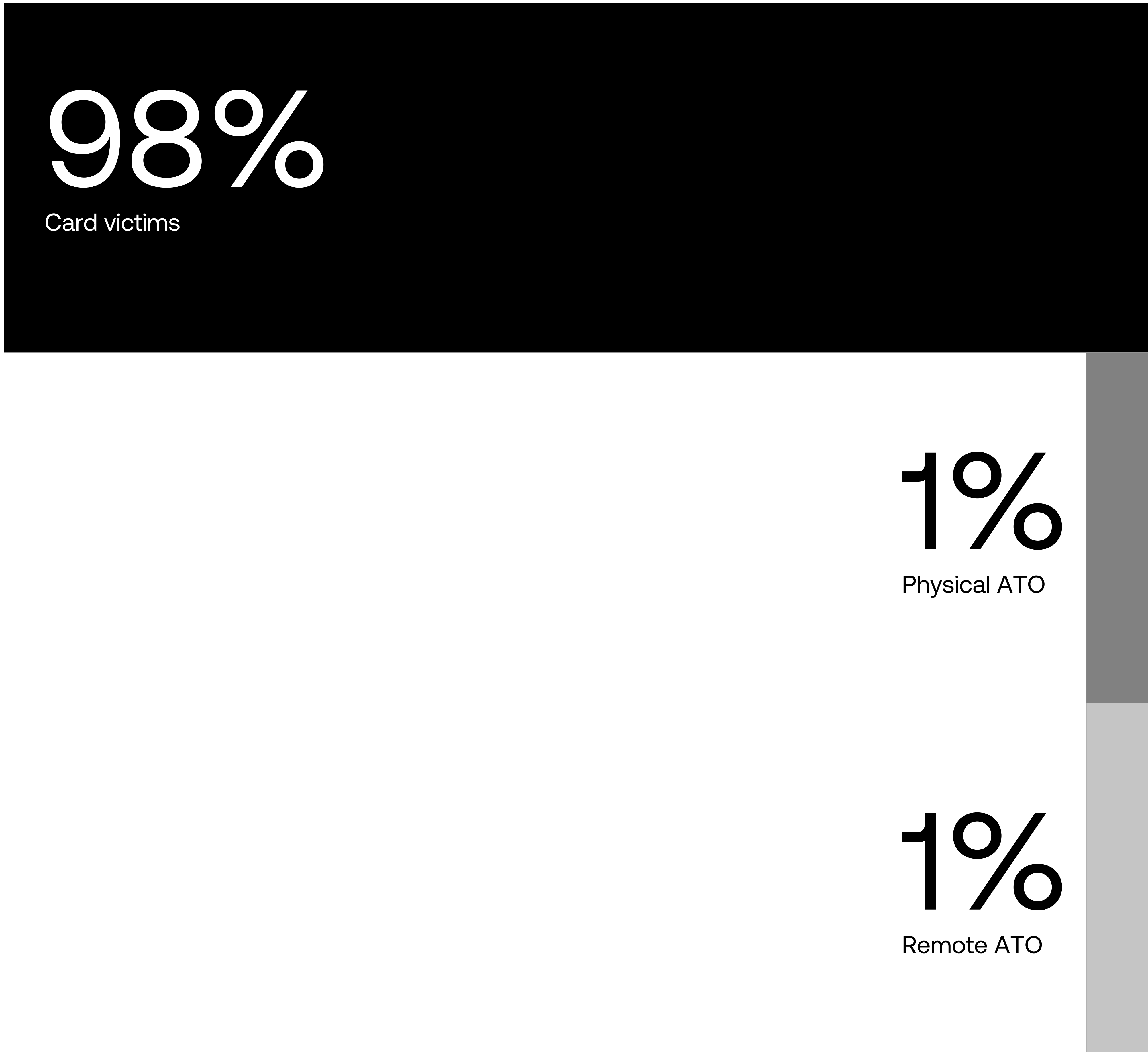
Over 95% of unauthorised fraud victims in the first half of 2024 were impacted by card fraud. But while it may be the most prevalent type, the average loss per customer in these instances continues to decline — between December 2023 and June 2024, it has dropped by 20%.

Preventative measures embraced by both Revolut and the broader financial services industry — like disposable, virtual cards meant for one-time use — have undoubtedly contributed to this decrease we're seeing.

With more data and personal information stored on mobile devices, it's no surprise that common thieves are increasingly targeting phones to access valuable data. However, despite these attempts, the incidence of this type of fraud continues to decline.

This reduction is largely due to the swift response from the industry, which has effectively addressed the growing threat of physical theft. Biometric technology, such as facial recognition and fingerprint security, has become a key solution where traditional passwords may fail. These advanced security measures provide robust protection for financial interests in cases of physical device theft.

◉ Exhibit 14 - Unauthorised Fraud (% of victims)



HOW REVOLUT IS FIGHTING FRAUD

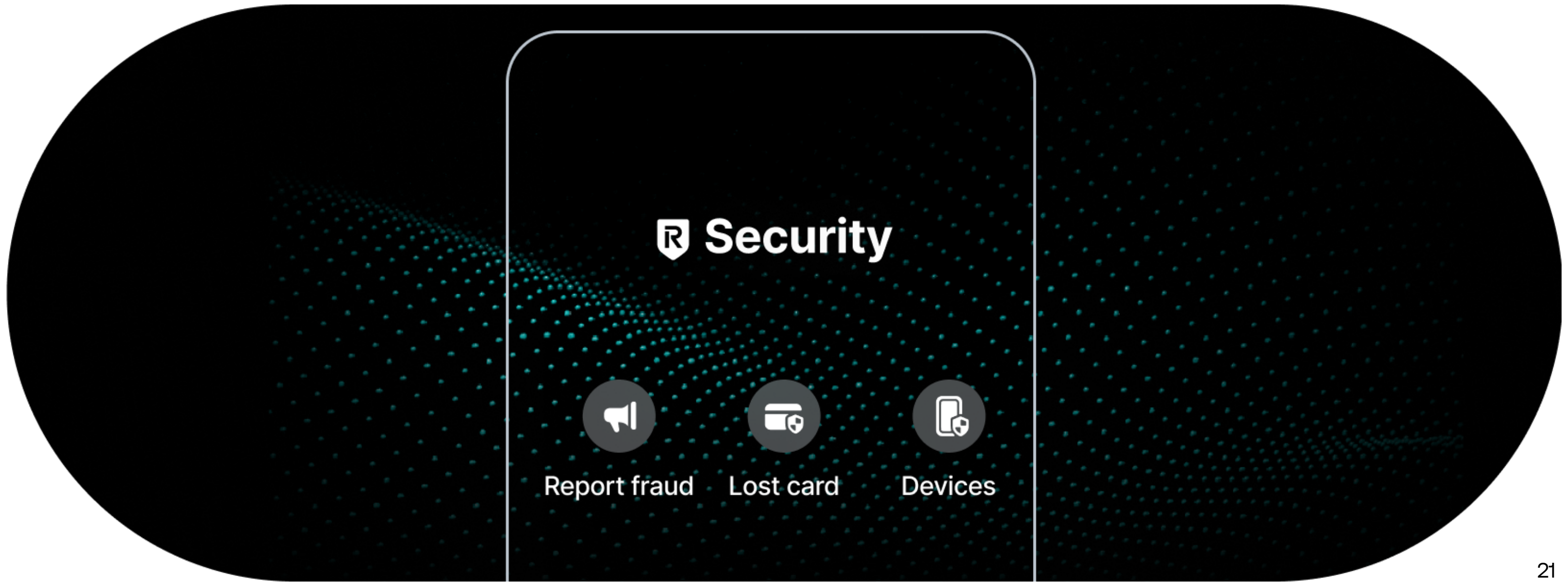
How Revolut protects its customers

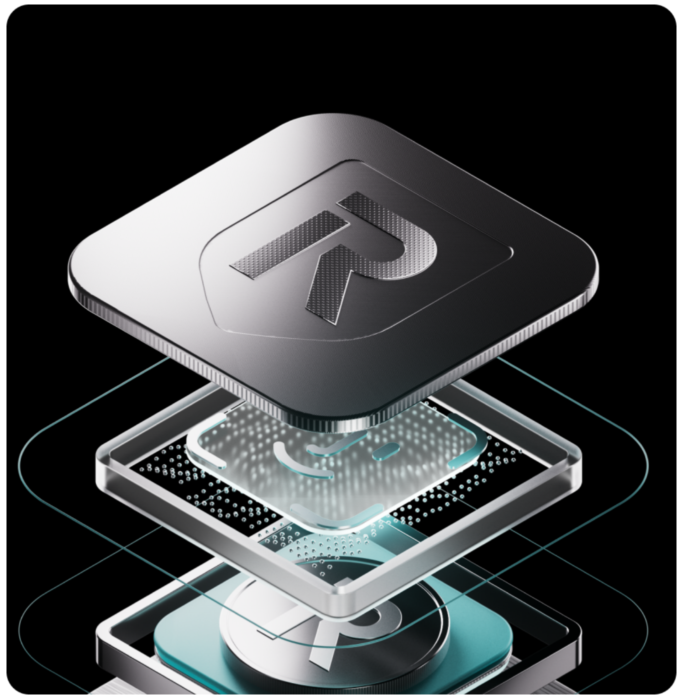
At the forefront of Revolut's security measures is its proprietary fraud detection system, employing cutting-edge machine learning and artificial intelligence methodologies. Revolut estimates that in 2023, it prevented over £475 million in fraud against its customers. This robust system meticulously analyses an impressive volume of up to 341 million customer transactions each month, actively searching for indicators of potential fraud. Staying ahead of the dynamic fraud landscape, Revolut continually monitors its evolution and responds swiftly by implementing enhanced customer security features:

● Exhibit 15 - Revolut's Wealth Protection feature in action

Wealth protection

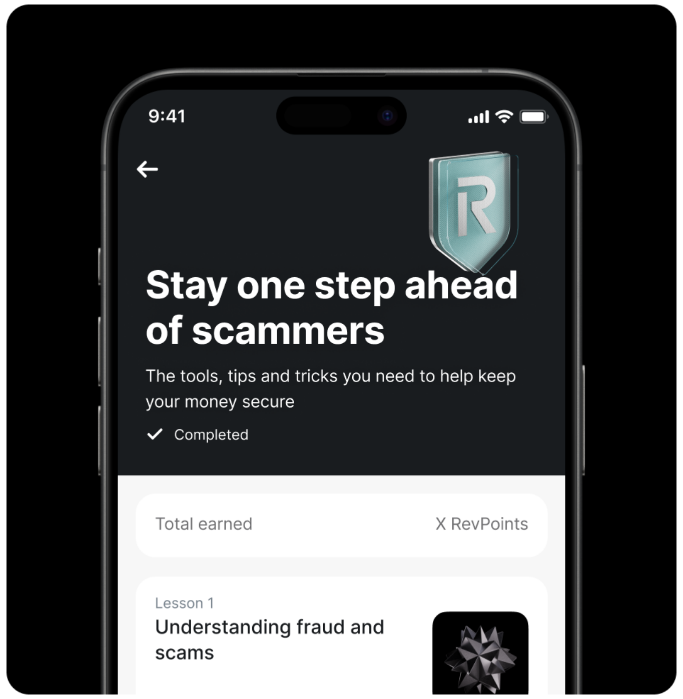
Revolut allows users to set up biometric authentication for withdrawals from their investments, as an extra layer of protection. Once enabled, all withdrawals from the following savings and investments will require selfie verification: Savings, Personal Pockets, and crypto trades and transfers.





Biometric interventions to protect customer funds in cases of physical theft

In the event a customer's device or credentials are stolen, Revolut's fraud detection machine learning models leverage biometrics to verify customers' identity for transactions that are deemed risky.



9:41

Stay one step ahead of scammers

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

✓ Completed

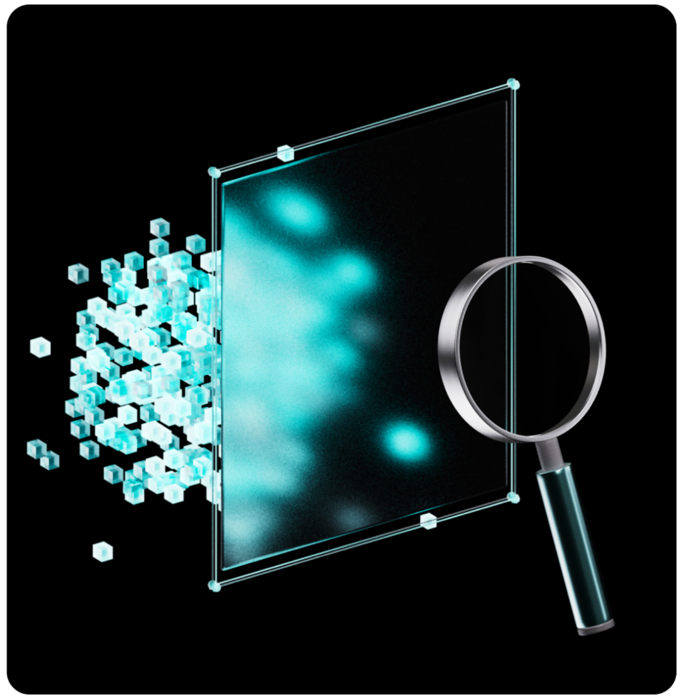
Total earned X RevPoints

Lesson 1

Understanding fraud and scams

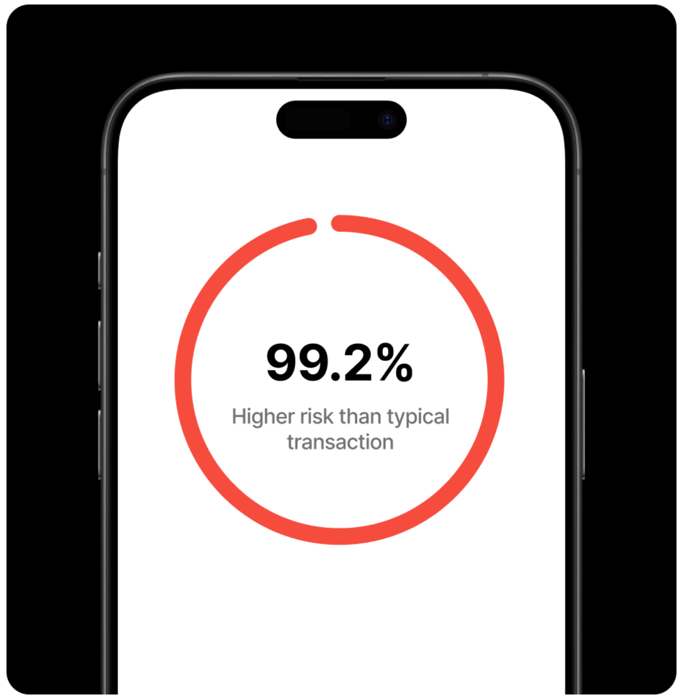
Elevating scam education through comprehensive initiatives

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



Delayed send functionality

To tackle the increase in authorised fraud, we delay transactions that are deemed risky, allowing users extra time for further consideration before they proceed with a transaction.



99.2%

Higher risk than typical transaction

Early warning systems and quick response yield results for authorised fraud

Revolut continues to adapt scam warnings and guidance as new trends, such as job scams, emerge. Revolut's dynamic fraud intervention models identify likely scams before payment is completed, cautioning users with signs to identify likely scams. Revolut also instituted targeted in-app chat interventions, requiring a customer to speak with a Revolut specialist before continuing. These interventions can uncover scam-specific red flags, and in 90% of cases are able to prevent fraud (Source).

CONCLUSIONS

The key findings in this report demonstrate that authorised fraud has been steadily increasing over time, accounting for a growing proportion of fraud cases.

Consumers are increasingly at risk to sophisticated scams, ranging from purchase and job scams to investment schemes — and the common underlying factor across these scams is their prevalence on social media platforms, particularly those owned by Meta.

At Revolut, we're fully committed to meeting this threat head on. Through a combination of advanced security features, enhanced customer protections, and our expanding team of financial crime experts, we are doing everything within our power to safeguard our customers.

However, the fight against fraud cannot be won by one organisation alone, nor should it be addressed only after a scam's success. It requires a concerted effort from unified governments, social media companies, and financial institutions to address these issues at their source and develop more effective countermeasures. Financial institutions should be the last — not the only — line of defence against fraud

Social media platforms must take a more active role in preventing fraud before it reaches consumers. This means implementing stronger safeguards, monitoring suspicious activity, and collaborating with financial institutions and governments to address these issues head-on, and not wait for the general public to fall victims of scams.

As these efforts continue, we remain steadfast in our dedication to deliver good outcomes to our customers, and educating global citizens about the increasing risk of financial fraud. We encourage them to stay vigilant and cautious, recognising the ever-present risks in today's connected ecosystems.

By working together, we can help mitigate the dangers and build a safer financial future for all.

Revolut

Revolut Group Holdings Ltd
Registered number: 12743269