Revolut

FINANCIAL CRIME AND CONSUMER SECURITY REPORT 2023

Contents

Introduction

Woody Malouf, Head of Financial Crime at Revolut on the inaugural Financial Crime and Consumer Security Insight Report:

Today we are publishing, for the first time, our Financial Crime and Consumer Security Report. The aim of this report is simple; to shed light on the intricate web of financial scams and frauds which pose increasing threats to individuals around the globe. This report details the types of fraud most prevalent in the market; highlights the Revolut data that supports this; showcases the work being done by Revolut to stop fraud and protect customers; and provides useful tips customers can use to protect themselves from these ruthless criminals. Fraud is an industry wide problem, impacting people and financial institutions across the globe, so our ultimate goal is to spread awareness and enhance the protection of everyday people.

Fraud has grown exponentially over the last few years at a global scale. In fact, over USD $1 trillion was lost to scams worldwide in 2022, according to a study carried out by the non-profit organisation Global Anti-Scam Alliance. There is no silver bullet, nor any one institution that can solve the fraud problem. But with the right people and technology in place, financial institutions can fight back and hold at bay these ruthless criminals.

Revolut invests heavily in the safety and security of its customers, protecting them from many types of fraud and scams. Our 2,500-strong, 24/7 financial crime team employs advanced AI-based algorithms, along with biometric tools and cybersecurity measures which in 2023 prevented over £475m of potential fraud against our customers.

To counter the ever changing tactics of fraudsters, Revolut is constantly strengthening its set of advanced, AI-based tools and techniques to prevent, detect, and disrupt fraudulent activity. The technology used by fraudsters to con innocent people is incredibly sophisticated and therefore our systems need to be even more so. There is an “arms race” taking place between financial institutions and fraudsters, and we are constantly evolving to win this. We are as committed as ever to protecting our customers from the fraudsters of today, as well as tomorrow.

As a global fintech, Revolut meticulously documents the type of fraudulent transactions that are recorded on its systems. This is done in order to better understand, and and in the future prevent fraud so that Revolut, as well as other financial institutions, can better protect our customers in the future.

This report sheds light on the type of fraud Revolut recorded in 2023 and the key takeaways from that data.

More specifically, the report examines Revolut data across its markets on:

- **Authorised vs Unauthorised Fraud**
- **Authorised Fraud**
  - Blackmail
  - Impersonation Scam
  - Invoice Scam
  - Investment Scam
  - Job Scam
  - Loan Scam
  - Purchase Scam
  - Relationship Scam
  - Tax Scam
- **Unauthorised Fraud**
  - Card fraud
  - Phone/Device theft
  - Account takeover
- **Social Media origins**
- **Country specific data**

What is fraud?

Fraud is grouped into two overarching categories: Unauthorised Fraud (also known as a “Fraud”) & Authorised Fraud (also known as a “Scam”).

- **Unauthorised Fraud/Fraud** occurs when sophisticated individuals aim to access others' money, sensitive information, or valuable assets, often by impersonating someone else. This type of fraud involves a fraudster gaining unwarranted access to someone's personal details. These fraudsters may use the stolen information to hijack accounts, conduct unauthorised payments, or apply for credit cards under the victim's name.

- **Authorised Fraud/Scam** are tricks or traps set by fraudsters. Authorised Fraud involves deceptive practices where individuals might encounter seemingly amazing deals or encounter imposters posing as trusted entities. These scammers utilise various methods, including fake phone calls, texts, emails, or social media posts, to convince people to make payments or transfer money to the fraudster’s account.

Types of Unauthorised Fraud

There are many types of Unauthorised Fraud. The three key ones customers are often exposed to are:

- **Physical Theft** - This is when fraudsters steal the device or phone that holds a customer's banking apps and are then able to to make payments or transfer out funds.
- **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, often using third-party software downloaded by the user.
- **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 (or Scams) are categorised based on the specific tactic used to defraud the customer. Here are common fraud tactics and how they work:

- **Purchase Scams**: This is the oldest trick in the book, and still popular today. Scammers trick victims with bogus websites that promise unrealistically low-priced products that are not 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. 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.
- **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.
- **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.
- **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.
- **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.

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

- **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.

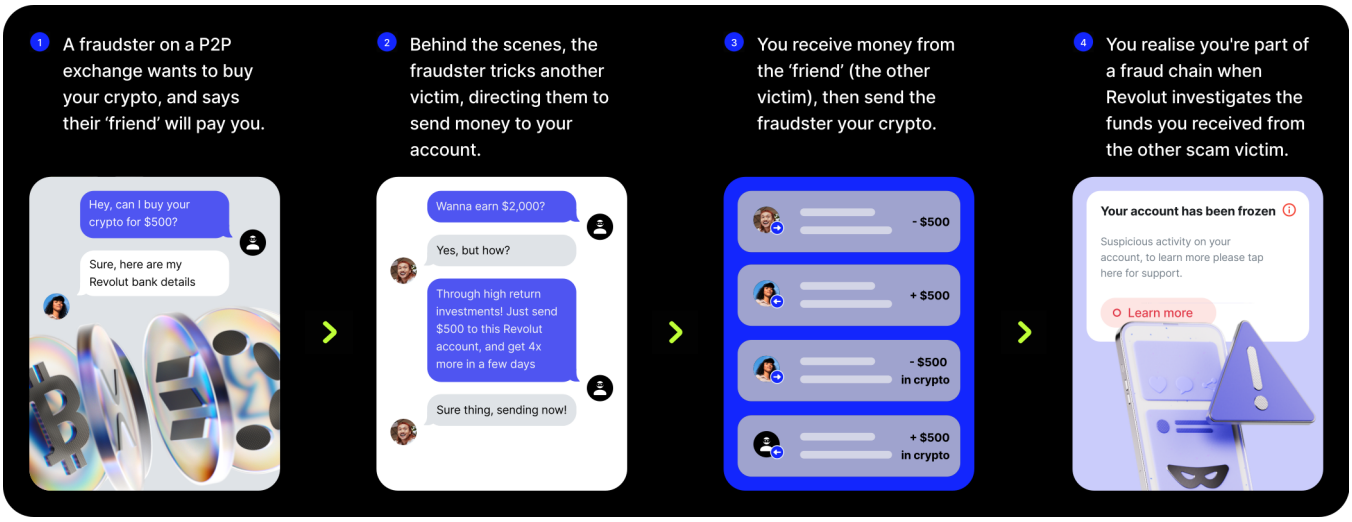
- **Blackmail:** Fraudsters threaten to expose private details or data, threaten loved ones, or cyber bully victims into making payments.

Authorised Fraud can also be grouped into two categories, based on the payment method used: Card Fraud and Authorised Push Payment Fraud (APP). This distinction is useful for the industry, as bank transfers are hard to trace, and victims have limited chances of getting their money back.

Other types of fraud

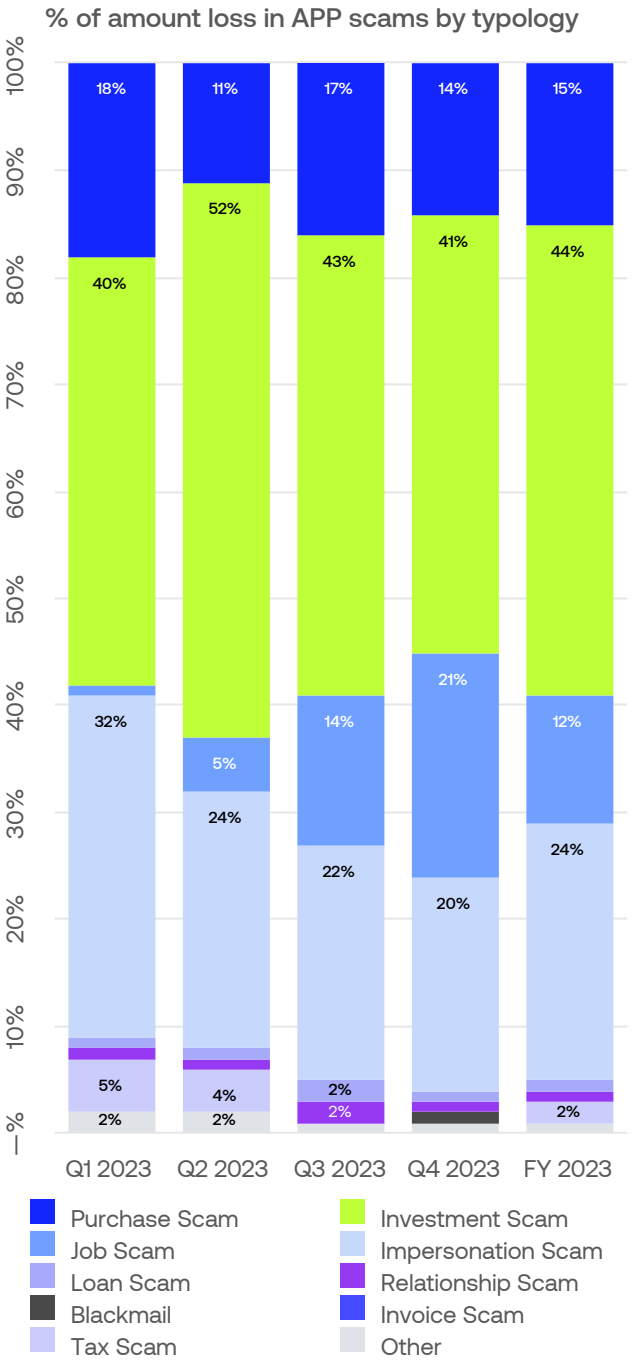
Triangle Scams are a combination of two or more types of scam, used by fraudsters to avoid detection. In triangle scams, there are two victims; Victim A is defrauded into making a payment to Victim B's account, and Victim B is subsequently defrauded into making a second likely bigger payment to the fraudster's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

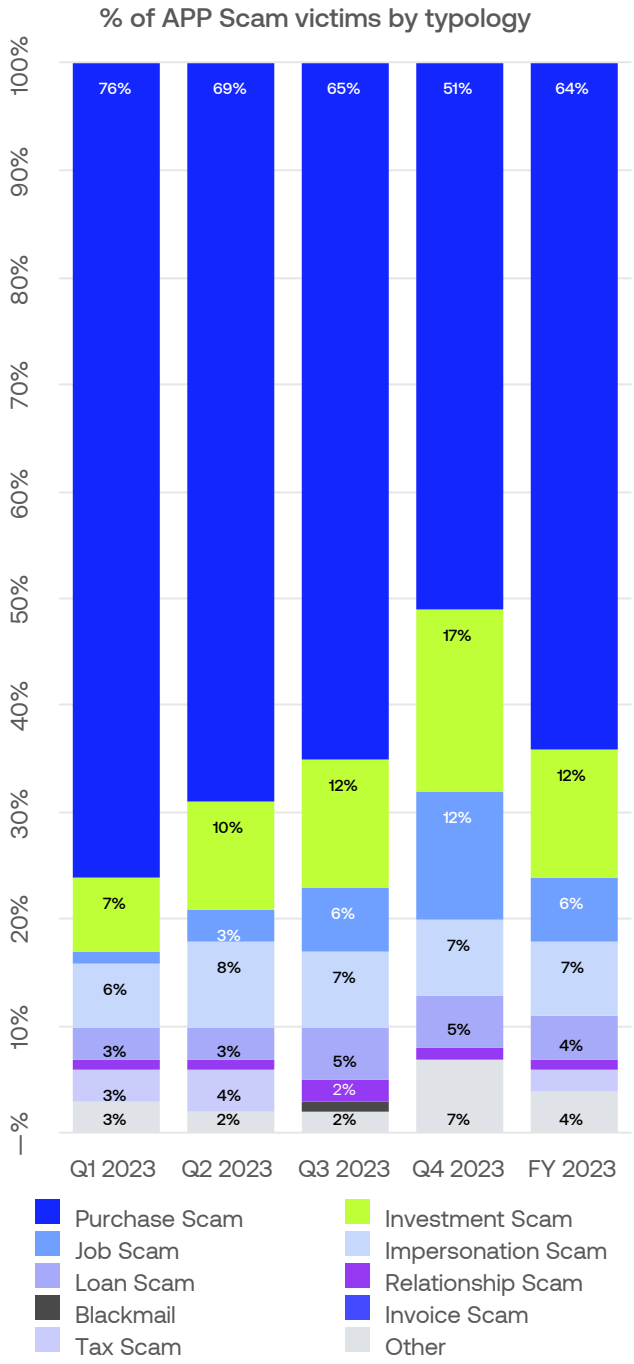
Here's an example of how a triangle scam combining two investment scams may operate:



2023 Global fraud & scam trends

Authorised Fraud





Key findings

Job scams increased by 1,200% over the course of the year, the most of any type of scam, from a relatively little used scam:

The prevalence of job scams increased significantly in 2023. Job scams represented only 1% of all fraud cases, as well as 1% of the overall value of all money lost to scams in Q1 2023. By Q4 2023, these figures rose to 12% of all cases and 21% of the overall value lost to scams, increasing 1,200% and 2,100% respectively. Similar to other types of fraud, job scams target those looking for an opportunity to boost their earnings. As the cost of living and high inflation takes hold, we have found the number of reported job scams dramatically increase, with criminals preying on those seeking a legitimate way to better their, in particular young and often inexperienced job seekers.

Purchase scams were the most popular type of scam, constituting 64% of all reported scams in 2023, but their use is declining:

Purchase scams were the most reported scam across every Revolut market. However, we observed a notable decline in the number of reported purchase scams across 2023, dropping from 76% of all cases in Q1 to 51% by Q4. This was likely the result of improved fraud security, resulting in scammers looking for other methods to con victims. Additionally, purchase scams were usually small scams with lower monetary losses, representing only 15% of the amount lost to scams in 2023, despite being the most comms scam.

Investment scams are becoming more prevalent, increasing by 142% over the course of the year, accounting for the highest percentage of money lost to scams:

Investment scams accounted for the highest reported losses in 2023. Because of this, the prevalence of this scam increased, with investment scams representing 7% of all reported cases in Q1, but growing to 17% in Q4. We observed that social media platforms in particular were a considerable driver for investment scams, with 58% of all money lost to scams that originated on Meta platforms.

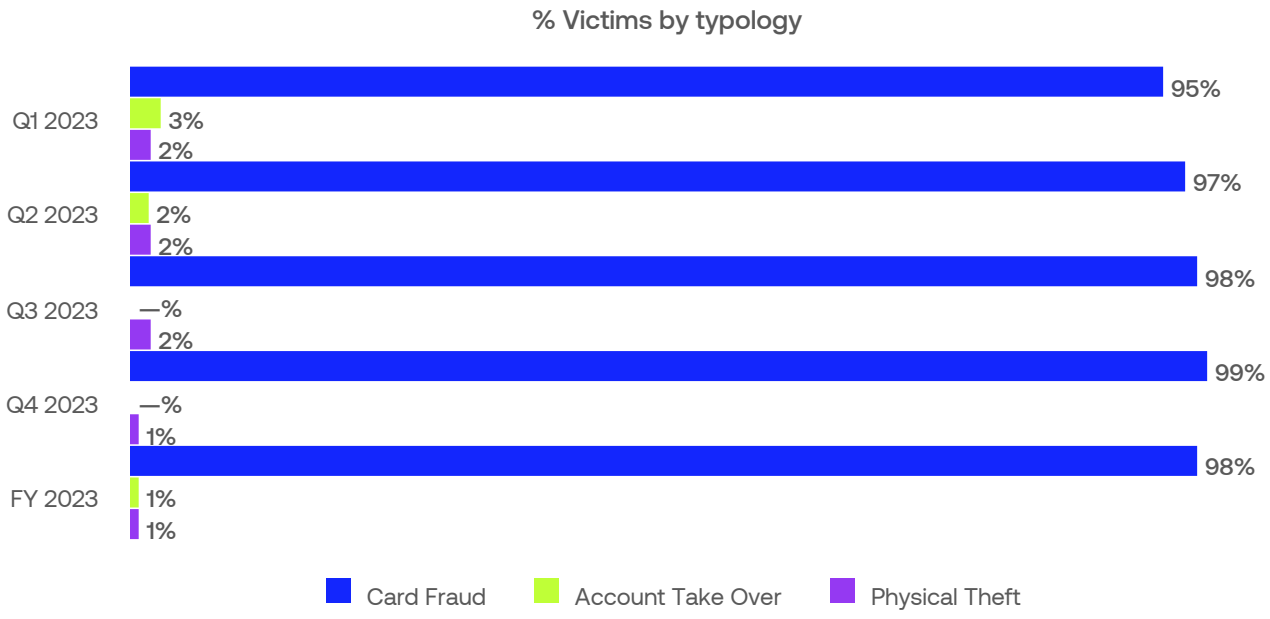
Impersonation scams saw a notable and consistent drop in money lost to this scam over the course of 2023:

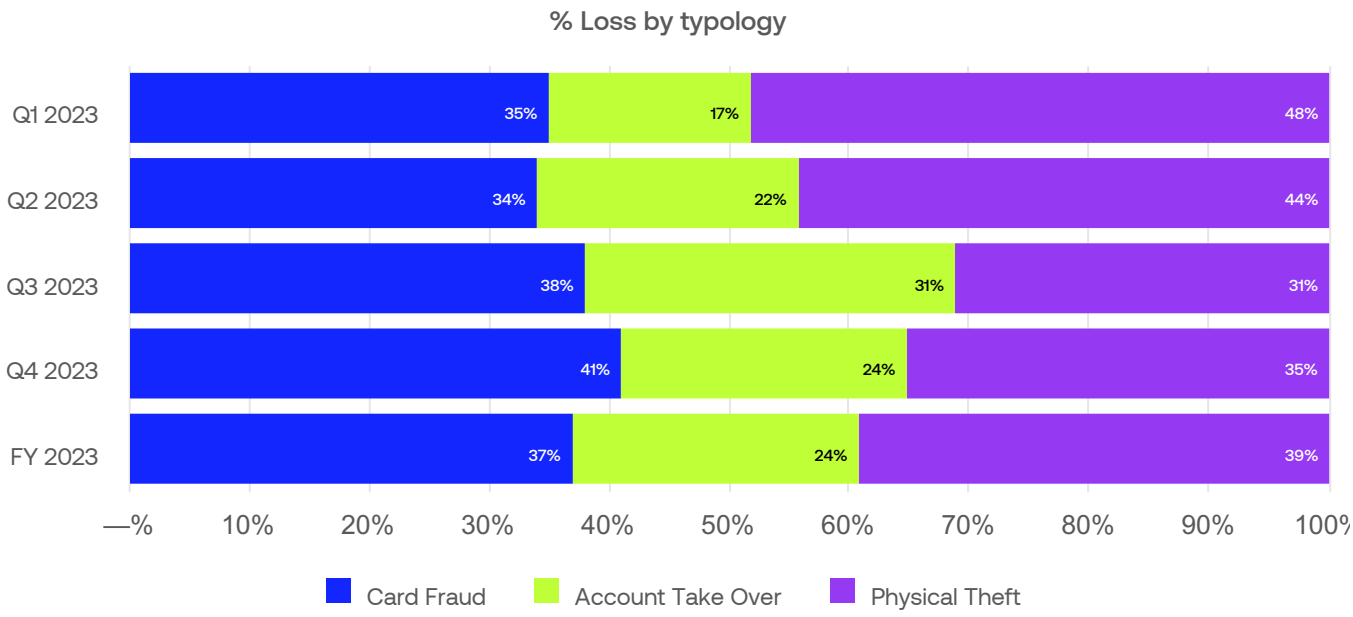
Whilst impersonation scams consistently made up between 5-7% of reported fraud cases in 2023, the percentage of money lost to this scam drop throughout the year. In Q1 2023, impersonation scams made up 32% of money lost to scams, before dropping to 20% in Q4 2023, a 37% drop over the course of the year. This was likely the result of improved customer education against this type of scam, resulting in scammers looking for other methods to con victims.

Tax scams are no longer a a prevalent scam type, decreasing significantly by the end of 2023:

The number of tax scams in 2023 dropped from 4% to less than 1% of total reported cases by the end of 2023. Customers have become more savvy to spotting tax scams, with threats of imprisonment by fake officials failing to have a notable impact.

Unauthorised Fraud





Key findings

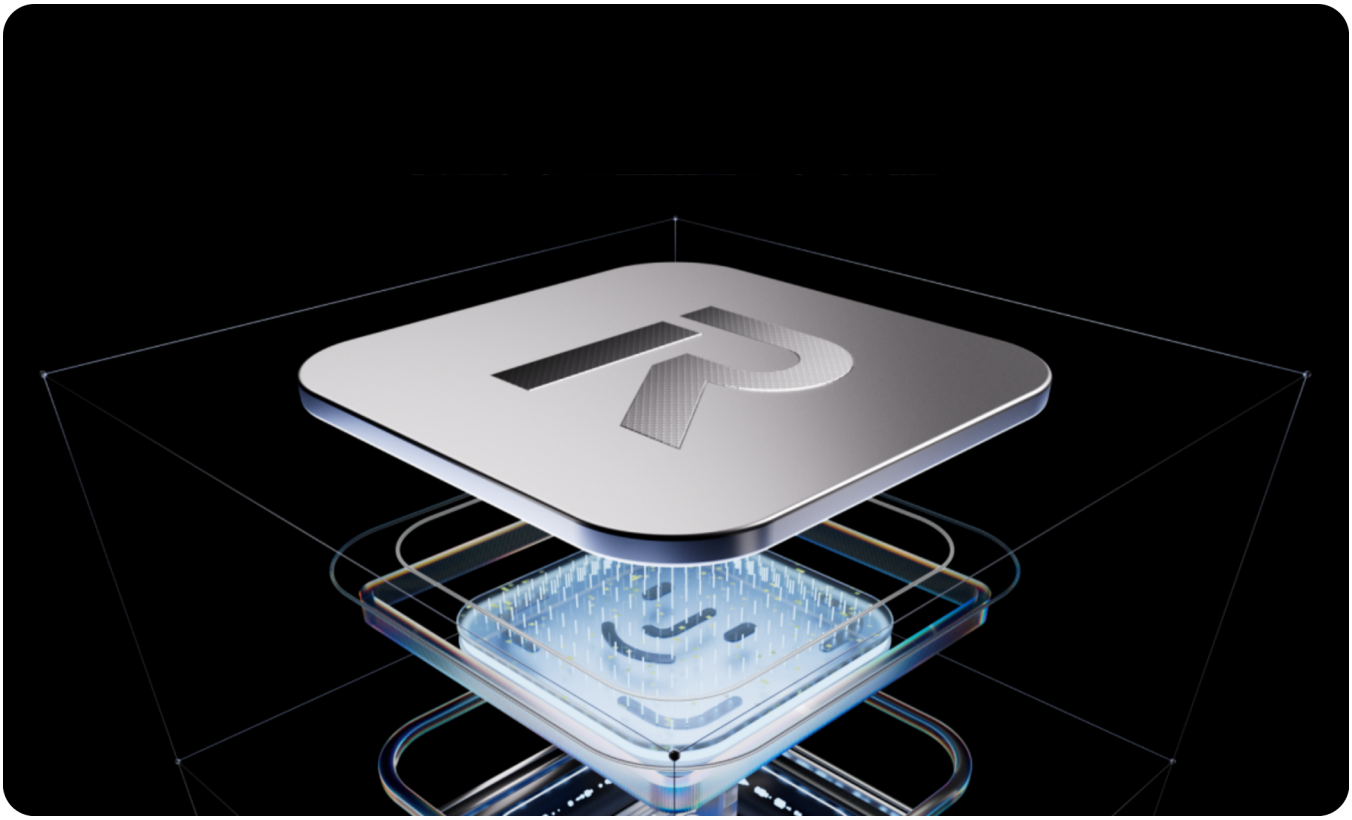
Physical Theft was responsible for 39% of all unauthorised fraud losses in 2023, despite only impacting 1% of total fraud victims:

With more and more data and information stored on mobile devices, it is no wonder that physical thefts result in the highest avg. loss per customer than any other fraud. Across the world, news outlets reported a surge in pickpocketing (USA[1], Netherlands[2], Spain[3]), with London in particular seeing a phone stolen every 6 minutes.[4]

Revolut has been swift to respond to the growing threat of physical theft, with biometrics at the forefront of the solution, where passwords fail. Biometric data such as face scans can be used to protect financial interests in the case of physical theft. Educating customers on the threat of physical theft has also become paramount, urging customers to remain vigilant to "shoulder surfers" and encourage users to regularly update their passcodes and not to use the same password across multiple applications.

98% of unauthorised fraud victims were affected by card fraud:

A common tactic for card information theft is Phishing: a form of cyber attack, delivered via email. These malicious messages typically appear to be from legitimate sources (such as banks, credit card companies, or online retailers) with the intent to collect personal and financial information. Disposable cards meant for one-time use have been adopted by the industry to reduce the risk of card fraud.



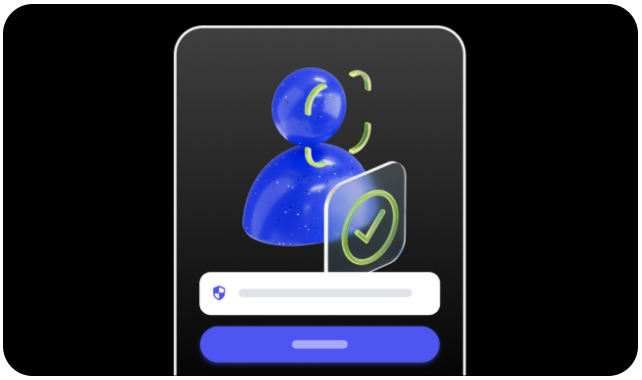
How Revolut is fighting fraud

Protecting our 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 potential fraud against its customers. This robust system meticulously analyses an impressive volume of up to 590+ 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:

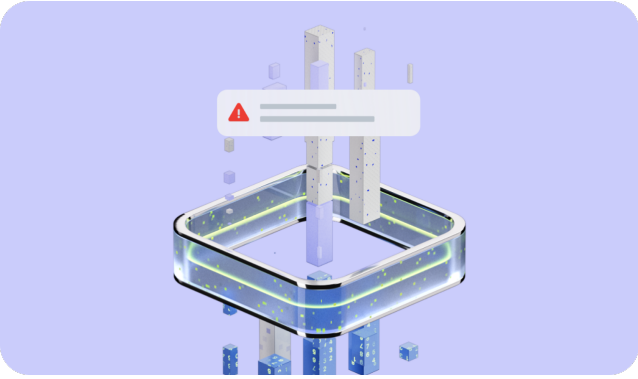
Virtual disposable cards protect against unauthorised card fraud

The single-use virtual cards can be used to shop online — and once a payment has been made, the details are destroyed so they can't be skimmed or re-used by criminals. Single-use virtual cards have fraud rates a third of that experienced with other cards, according to Revolut data. Learn more about virtual cards here.



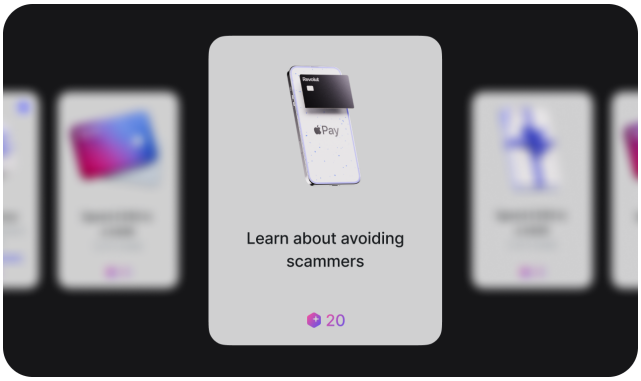
RAT detection technology

Biometric industry estimates[12] find that 12% of all fraud in EMEA comes from Remote Access Trojan (RAT) attacks. In comparison, at Revolut this share is less than 1%. Revolut's advanced machine learning-based monitoring systems and biometrics features limit fraudsters' access to funds in case of RAT attacks. This year, Revolut improved system capabilities to detect any compromised apps.



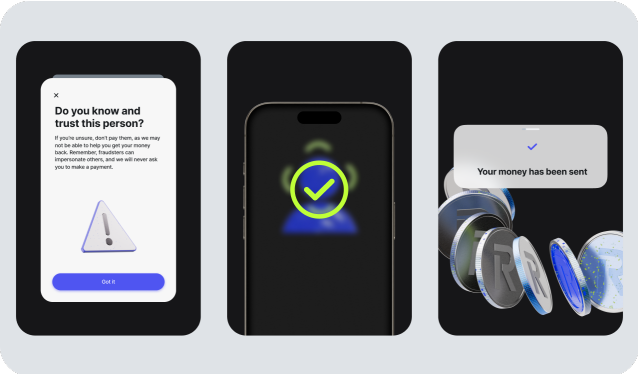
Flexible early warning systems against scams yield results

Revolut's dynamic fraud intervention systems identify likely scams before the payment is completed, using innovative approaches to break the spell. The system is highly responsive, with Revolut adjusting its transaction time warnings specifically to counter job scams as soon as they emerged as a major threat in August. These interventions can uncover scam-specific red flags, and in 90% of cases are able to prevent fraud.



Elevating scam education through comprehensive initiatives

Revolut's in-app Learn program now includes scam awareness campaigns, empowering customers with the knowledge and tools necessary to stay one step ahead of malicious actors.



Biometric interventions to protect user funds in cases of physical theft

Revolut's fraud detection machine learning models identify any risky transactions and leverage biometrics to verify customer identity for risky transactions. It offers a smooth selfie-check feature that ensures that even if someone gets a hold of your phone and password, your account with Revolut will be protected.

How to protect yourself from fraud

Here are a few tricks to stay one step ahead of scammers

1. **Stay alert.** Always question things that seem too good to be true.
2. **Trust your instincts**. If something feels off, take a step back and investigate.
3. **Use secure channels.** Stick to trusted websites and platforms for transactions.
4. **Report suspicious activity.** If something seems suspicious, let Revolut know — we're here to help 24/7, directly from the app.

How to identify a scammer

Scammers often use tricks to lure users into sharing personal information or moving their money. There are a few telltale signs, including:

- **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.

Fortunately, there are ways customers can protect themselves. Here's a checklist that customers can consult before they make any decisions about sending their money.

- **Research and verification**. Before sharing any personal details, customers should research the sender or company, check for contact details, read reviews, and verify with trusted sources.
- **Secure transactions.** Customers must use secure payment methods and verify the authenticity of the recipient.
- **Update the Revolut app.** This is essential for reinforcing Revolut protective measures. Customers can also enable auto-updates in their device settings to guarantee they are running the most secure version.

Something to remember: Revolut will only communicate through their official in-app chat support asking to move customer's money to a different account for safety reasons – never via phone. If Revolut needs to call a customer, they will only do so once they have scheduled it with the customer via the in-app chat.

- *For more information on fraud prevention, explore Revolut Online resources.*

References

- Global Anti-Scam Alliance (GASA) & ScamAdviser. (2022). 2022 Global State of Scams report.
- CBS News. (n.d.). NYPD pickpocket unit targets New York City holiday thefts.
- BBC News. (2023). London's fight against pickpockets.
- De Telegraaf. (n.d.). Zakkenrollers overspoelen de Nederlandse straten en evenementen.
- Ministerio del Interior, Gobierno de España. (2023). Estadísticas de criminalidad.
- Evening Standard. (n.d.). Stolen phone thefts in London: Password filming by thieves.
- BioCatch. (2023). EMEA Fraud Intelligence Annual Report 2023.

About the data

This report focuses exclusively on data pertaining to retail fraud reported in the calendar year 2023, unless specified otherwise. All analysis and findings are confined to fraudulent activities impacting retail customers being defrauded. Data on fraud involving business customers or acquiring fraud is not included in this report. The foundation of our report is data sourced internally from Revolut. Insights drawn are reflective of Revolut's consumer base and may not represent the broader industry. For the purposes of consistency, only fraud reported within 42 days is included in the report.

Appendix

Table 3.2.1

% of victims by typology of APP Fraud

APP Authorized Fraud	Q1 2023	Q2 2023	Q3 2023	Q4 2023	FY 2023
Other	3 %	2 %	2 %	7 %	4 %
Tax Scam	3 %	4 %	— %	— %	1 %
Invoice Scam	— %	— %	— %	— %	— %
Blackmail	— %	— %	1 %	— %	— %
Relationship Scam	1 %	1 %	2 %	1 %	1 %
Loan Scam	3 %	3 %	5 %	5 %	4 %
Impersonation Scam	5 %	8 %	7 %	7 %	7 %
Job Scam	1 %	3 %	6 %	12 %	6 %
Investment Scam	7 %	10 %	12 %	17 %	12 %
Purchase Scam	76 %	69 %	65 %	51 %	63 %

Table 3.2.2

% of amount lost by typology of APP Fraud

APP Authorized Fraud	Q1 2023	Q2 2023	Q3 2023	Q4 2023	FY 2023
Other	2 %	2 %	1 %	1 %	1 %
Tax Scam	5 %	4 %	— %	— %	2 %
Invoice Scam	— %	— %	— %	— %	— %
Blackmail	— %	— %	— %	1 %	— %
Relationship Scam	1 %	1 %	2 %	1 %	1 %
Loan Scam	1 %	1 %	2 %	1 %	1 %
Impersonation Scam	32 %	24 %	22 %	20 %	24 %
Job Scam	1 %	5 %	14 %	21 %	12 %
Investment Scam	39 %	52 %	43 %	40 %	44 %
Purchase Scam	18 %	11 %	17 %	14 %	15 %

Table 3.3.1

% of victims by typology of unauthorised Fraud

Unauthorised Fraud	Q1 2023	Q2 2023	Q3 2023	Q4 2023	FY 2023
Card Fraud	95 %	97 %	98 %	99 %	98 %
Account Takeover	3 %	2 %	— %	— %	1 %
Physical Theft	2 %	2 %	2 %	1 %	1 %

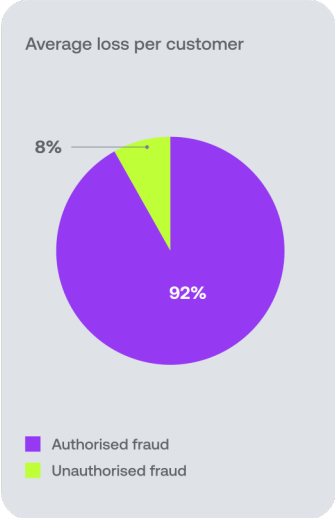
Table 3.3.2

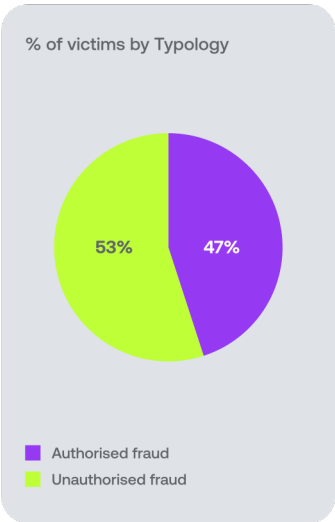
% of amount loss by typology of unauthorised Fraud

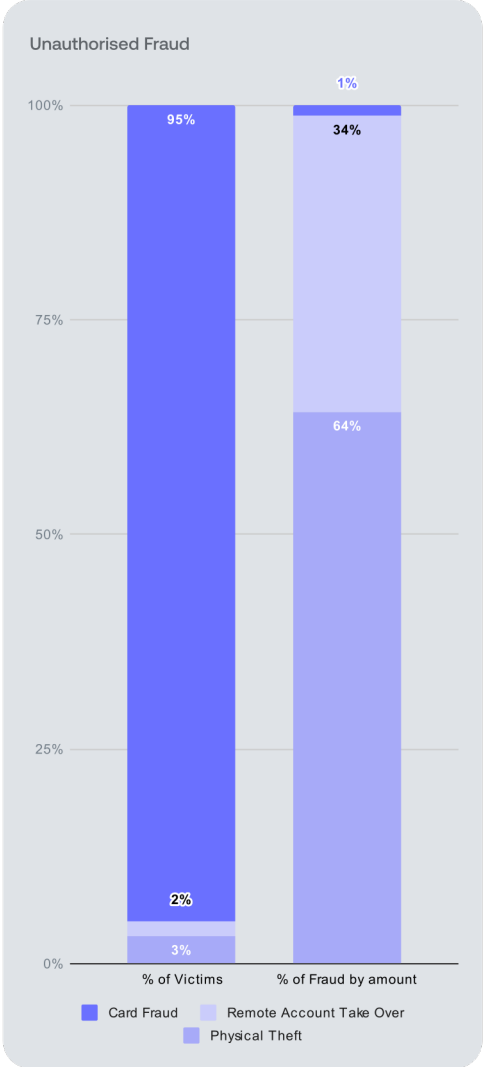
Unauthorised Fraud	Q1 2023	Q2 2023	Q3 2023	Q4 2023	FY 2023
Card Fraud	35 %	34 %	38 %	41 %	37 %
Account Takeover	17 %	22 %	31 %	24 %	24 %
Physical Theft	48 %	44 %	31 %	34 %	39 %

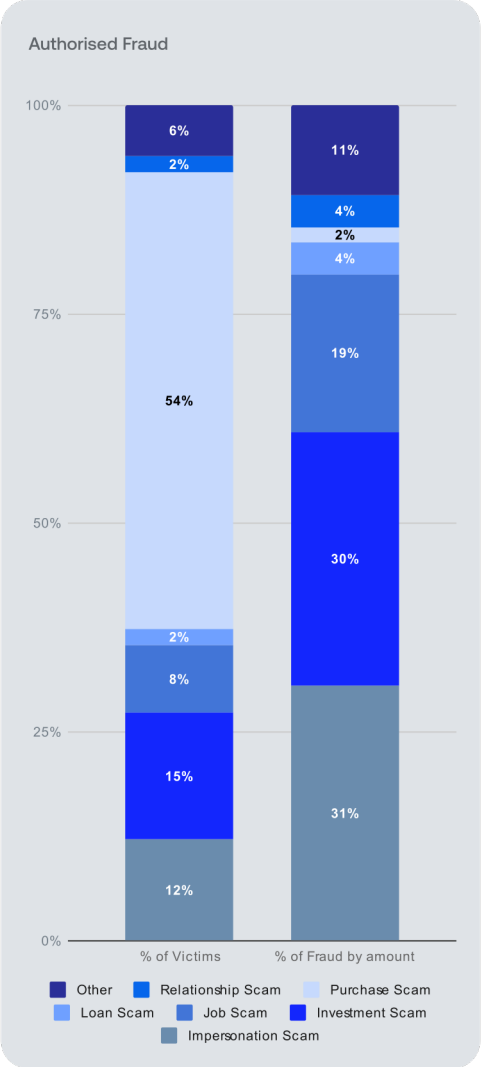
World Fraud Charts

UK

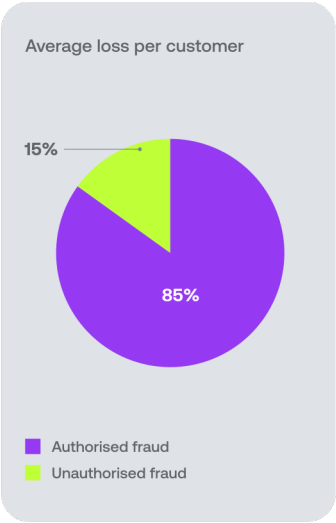


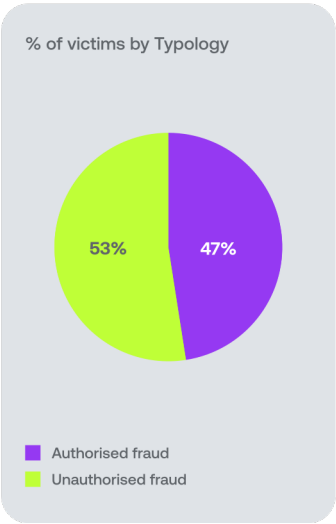


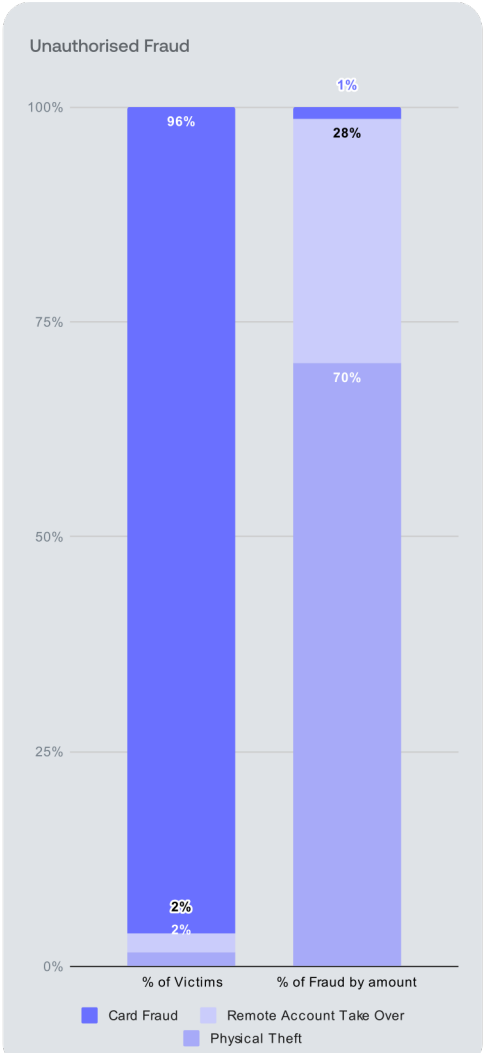


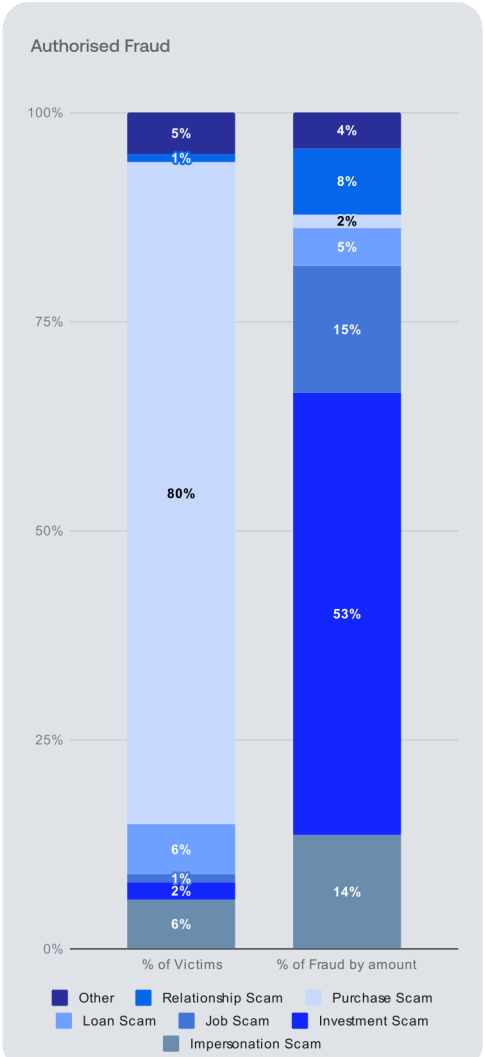


IRELAND


Average loss per customer
15%
85%
Authorised fraud
Unauthorised fraud

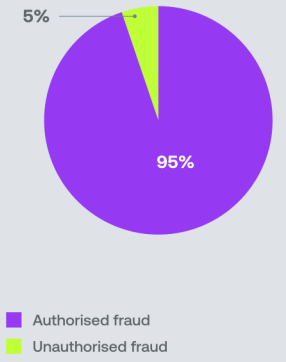

% of victims by Typology
53%
47%
Authorised fraud
Unauthorised fraud


Unauthorised Fraud
100%
75%
50%
25%
0%
96%
2%
2%
1%
28%
70%
% of Victims
% of Fraud by amount
Card Fraud
Remote Account Take Over
Physical Theft

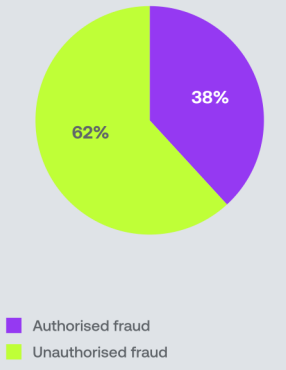

Authorised Fraud
100%
75%
50%
25%
0%
5%
1%
80%
6%
1%
2%
6%
4%
8%
2%
5%
15%
53%
14%
% of Victims
% of Fraud by amount
Other
Relationship Scam
Purchase Scam
Loan Scam
Job Scam
Investment Scam
Impersonation Scam

ROMANIA

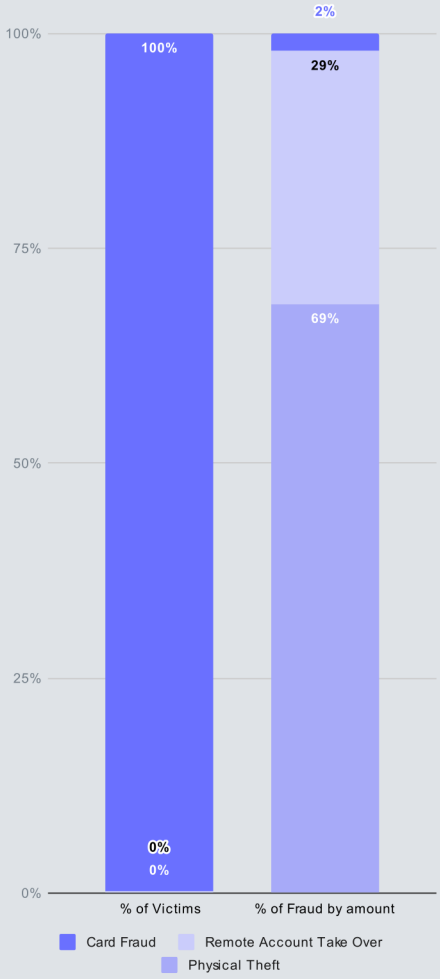
Average loss per customer



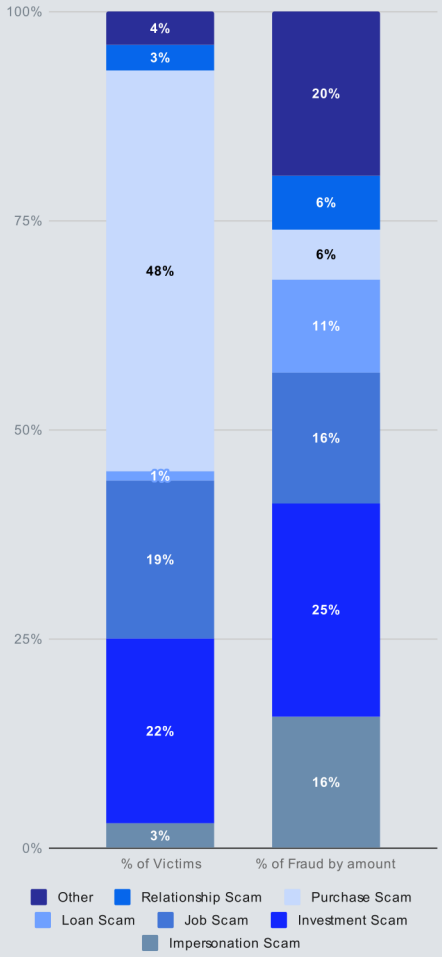
% of victims by Typology



Unauthorised Fraud

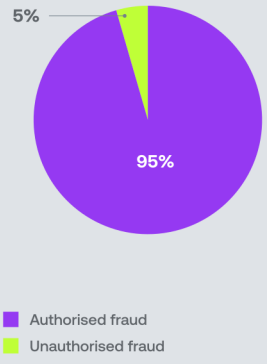


Authorised Fraud

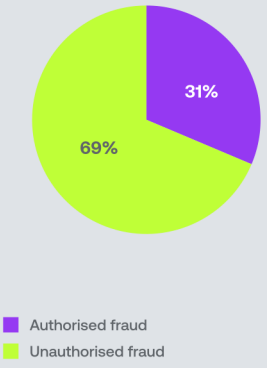


POLAND

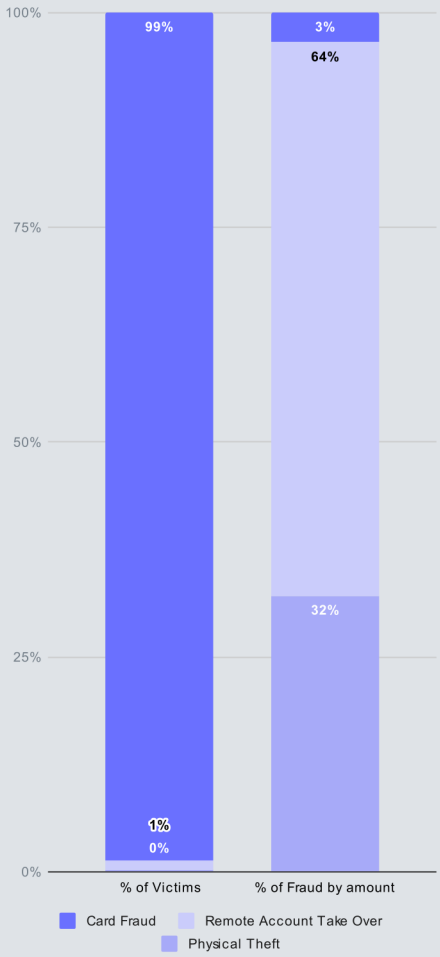
Average loss per customer



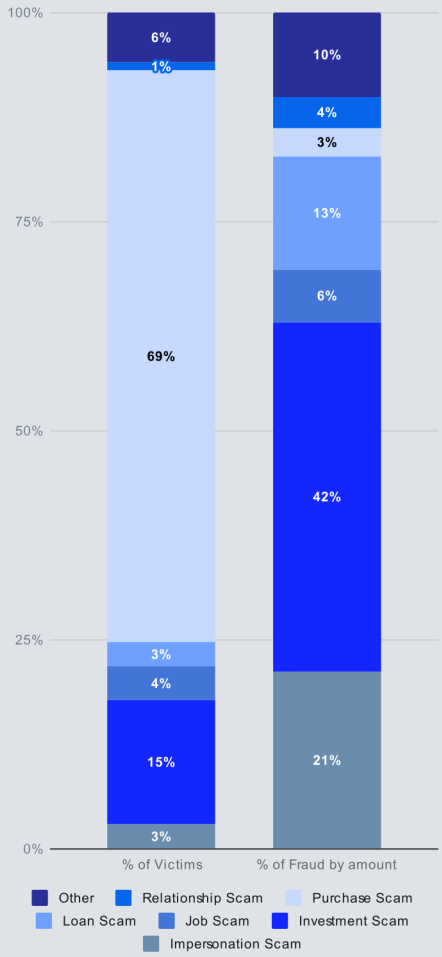
% of victims by Typology



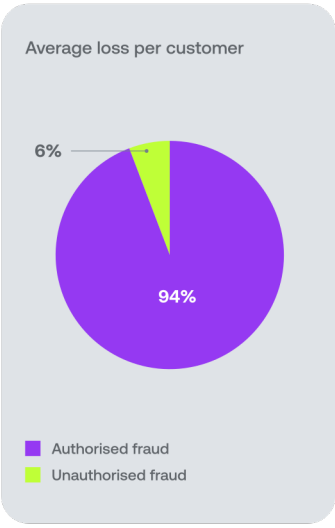
Unauthorised Fraud

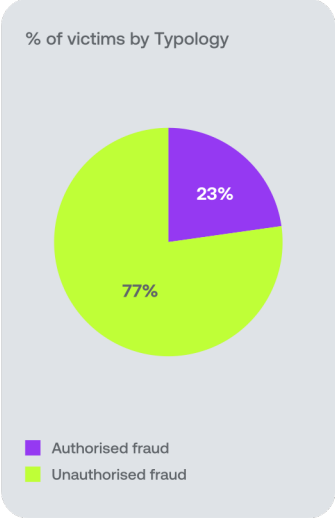


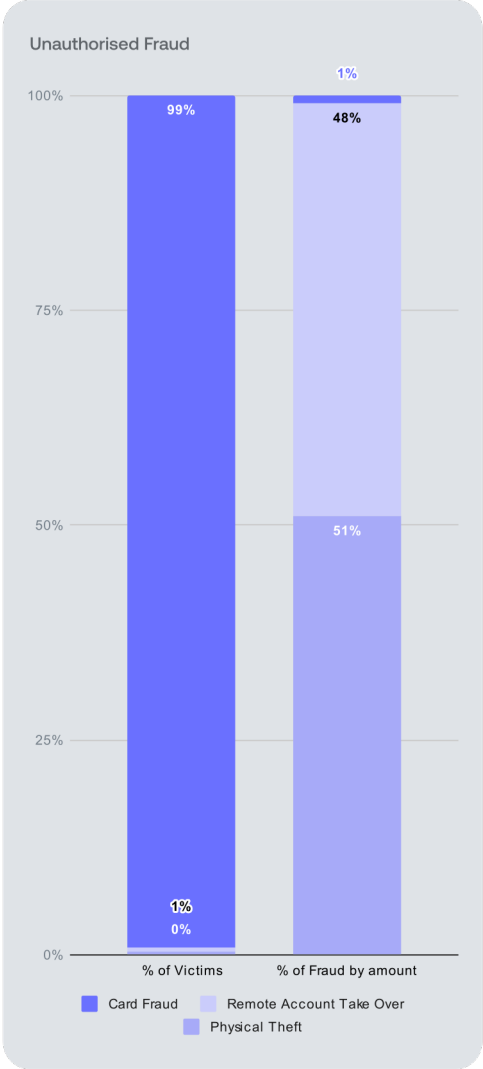
Authorised Fraud

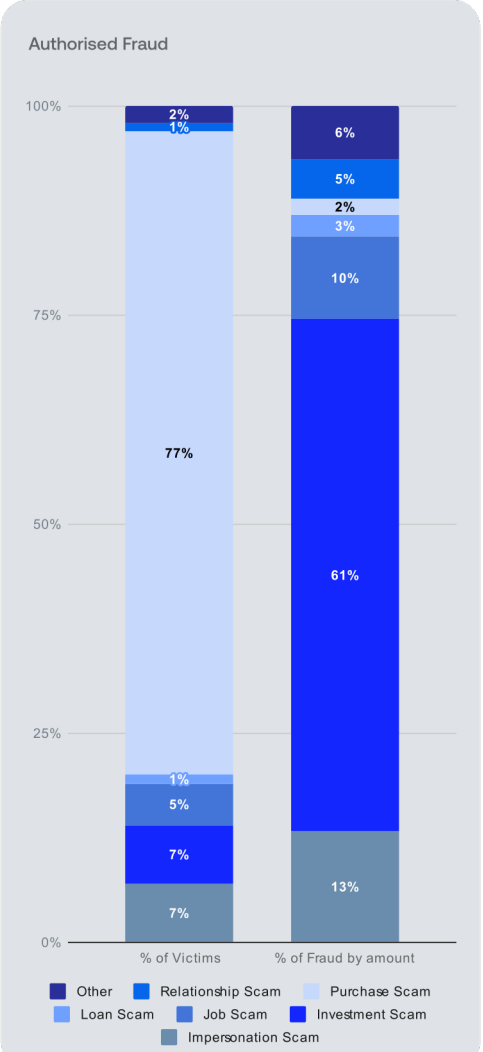


FRANCE

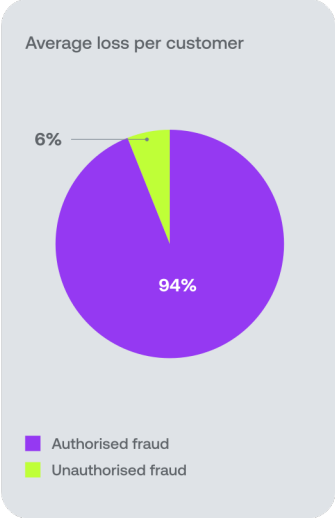

Average loss per customer
6%
94%
Authorised fraud
Unauthorised fraud

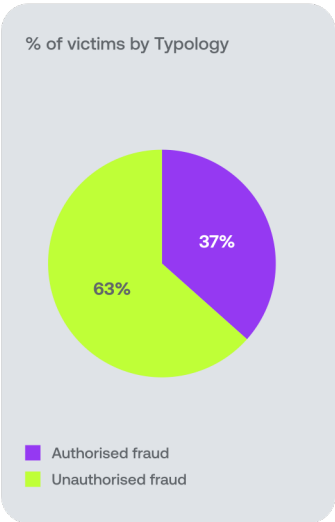

% of victims by Typology
23%
77%
Authorised fraud
Unauthorised fraud

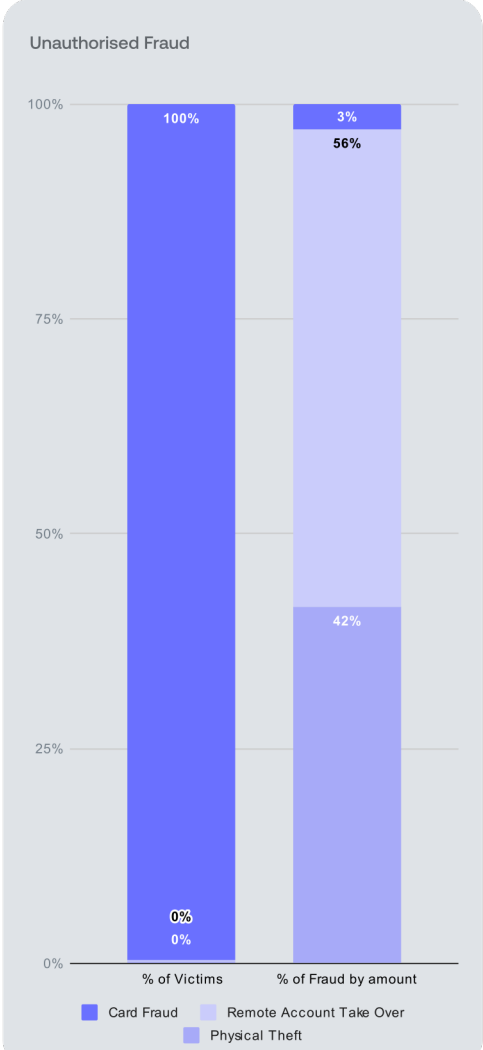

Unauthorised Fraud
100%
75%
50%
25%
0%
99%
1%
0%
1%
48%
51%
% of Victims
% of Fraud by amount
Card Fraud
Remote Account Take Over
Physical Theft

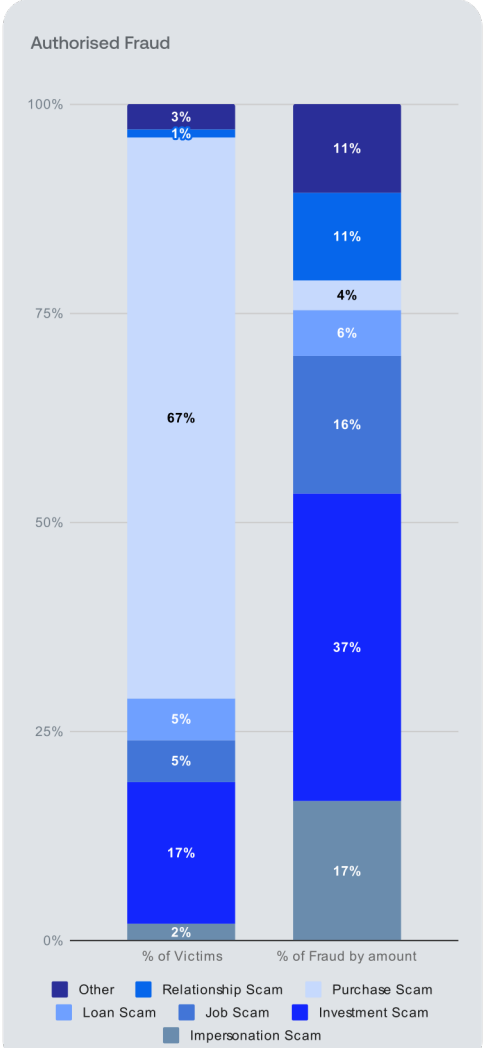

Authorised Fraud
100%
75%
50%
25%
0%
2%
1%
77%
1%
5%
7%
7%
6%
5%
2%
3%
10%
61%
13%
% of Victims
% of Fraud by amount
Other
Relationship Scam
Purchase Scam
Loan Scam
Job Scam
Investment Scam
Impersonation Scam

GERMANY

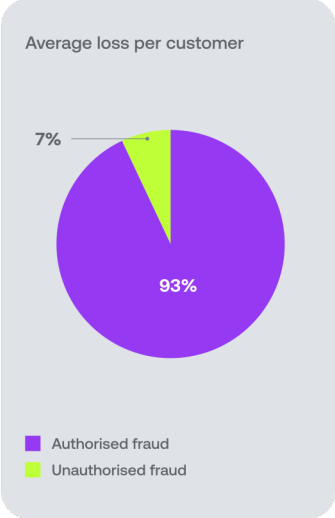

Average loss per customer
6%
94%
Authorised fraud
Unauthorised fraud

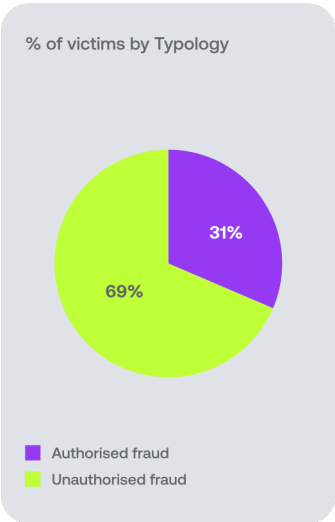

% of victims by Typology
37%
63%
Authorised fraud
Unauthorised fraud

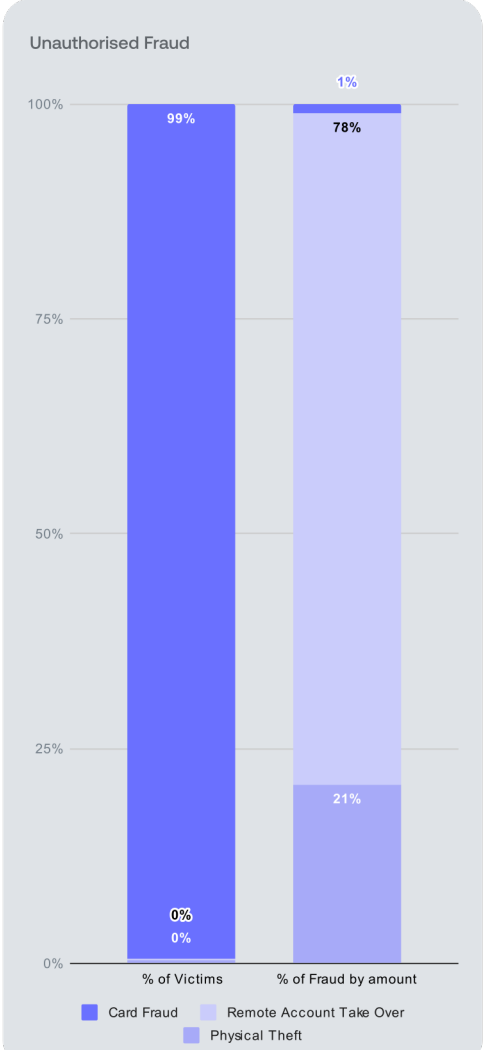

Unauthorised Fraud
100%
75%
50%
25%
0%
100%
0%
0%
3%
56%
42%
% of Victims
% of Fraud by amount
Card Fraud
Remote Account Take Over
Physical Theft

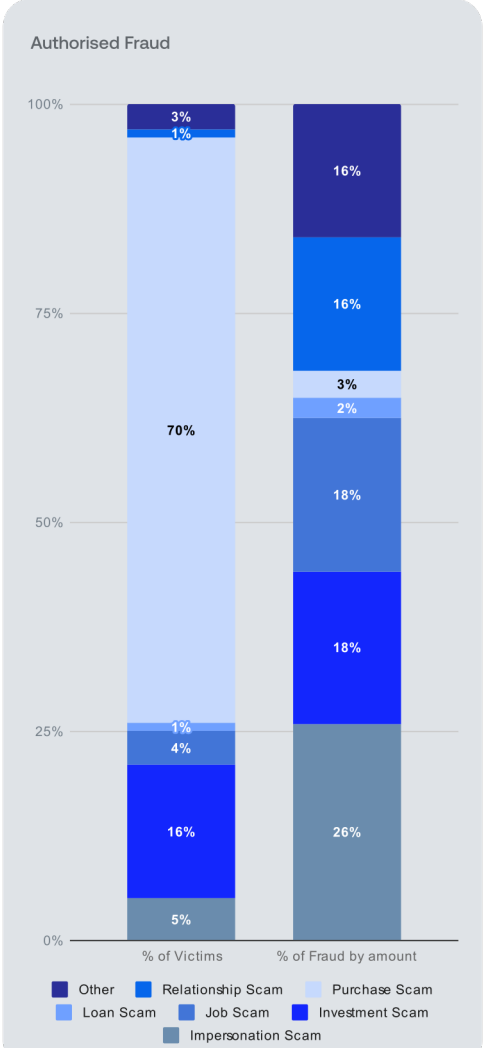

Authorised Fraud
100%
75%
50%
25%
0%
3%
1%
67%
5%
5%
17%
2%
11%
11%
4%
6%
16%
37%
17%
% of Victims
% of Fraud by amount
Other
Relationship Scam
Purchase Scam
Loan Scam
Job Scam
Investment Scam
Impersonation Scam

ITALY

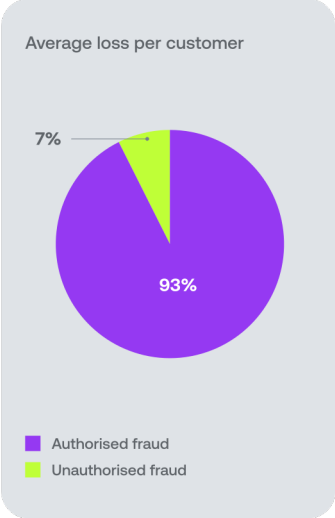

Average loss per customer
7%
93%
Authorised fraud
Unauthorised fraud

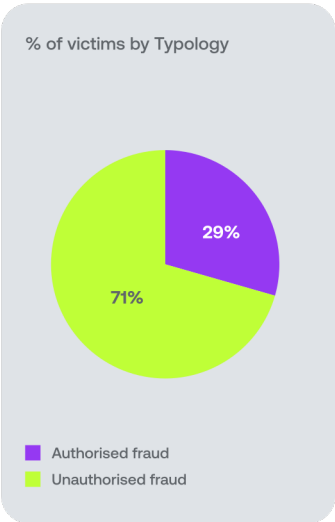

% of victims by Typology
31%
69%
Authorised fraud
Unauthorised fraud

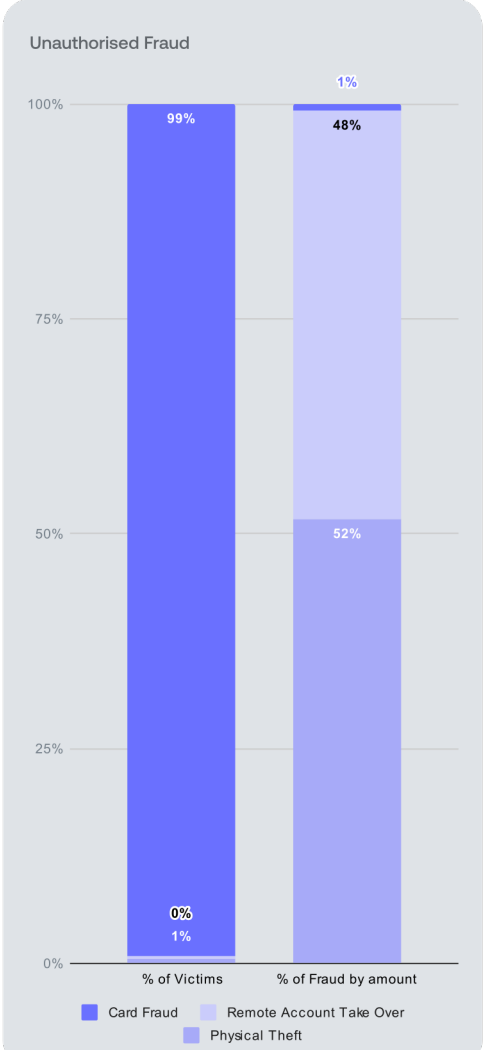

Unauthorised Fraud
100%
75%
50%
25%
0%
99%
0%
0%
1%
78%
21%
% of Victims
% of Fraud by amount
Card Fraud
Remote Account Take Over
Physical Theft

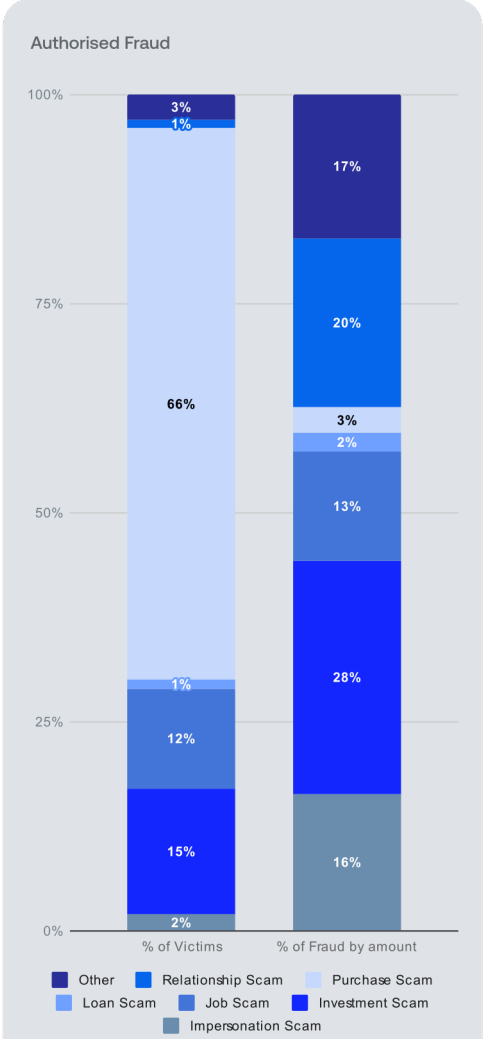

Authorised Fraud
100%
75%
50%
25%
0%
3%
1%
70%
1%
4%
16%
5%
16%
16%
3%
2%
18%
18%
26%
% of Victims
% of Fraud by amount
Other
Relationship Scam
Purchase Scam
Loan Scam
Job Scam
Investment Scam
Impersonation Scam

SPAIN


Average loss per customer
7%
93%
Authorised fraud
Unauthorised fraud

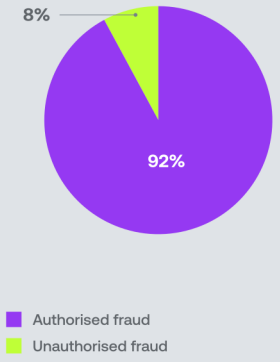

% of victims by Typology
29%
71%
Authorised fraud
Unauthorised fraud


Unauthorised Fraud
100%
75%
50%
25%
0%
99%
0%
1%
1%
48%
52%
% of Victims
% of Fraud by amount
Card Fraud
Remote Account Take Over
Physical Theft

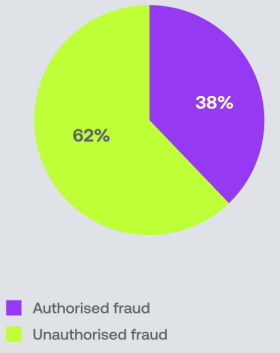

Authorised Fraud
100%
75%
50%
25%
0%
3%
1%
66%
1%
12%
15%
2%
17%
20%
3%
2%
13%
28%
16%
% of Victims
% of Fraud by amount
Other
Relationship Scam
Purchase Scam
Loan Scam
Job Scam
Investment Scam
Impersonation Scam

HUNGARY

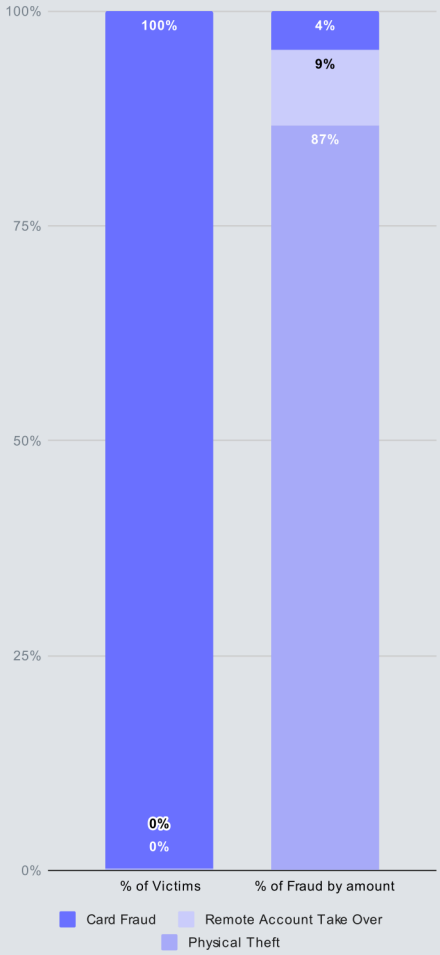
Average loss per customer



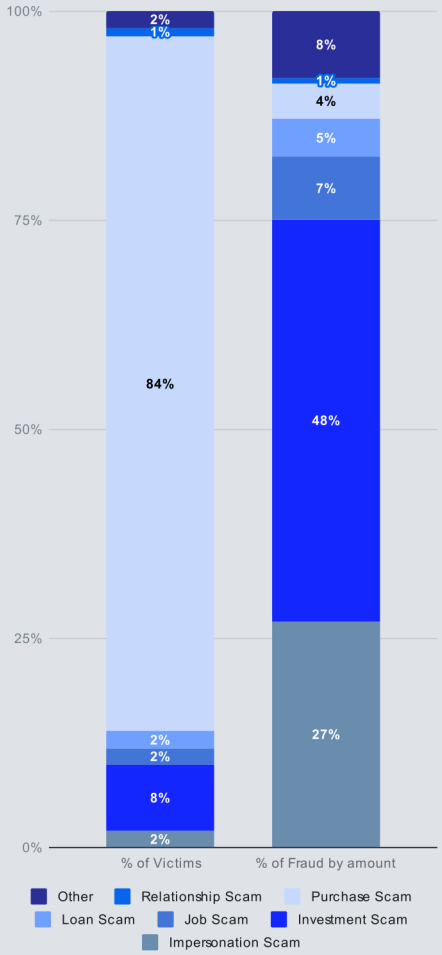
% of victims by Typology



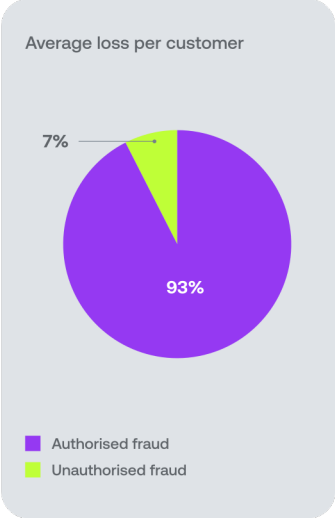
Unauthorised Fraud

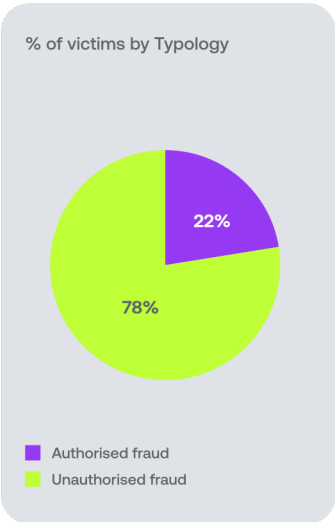


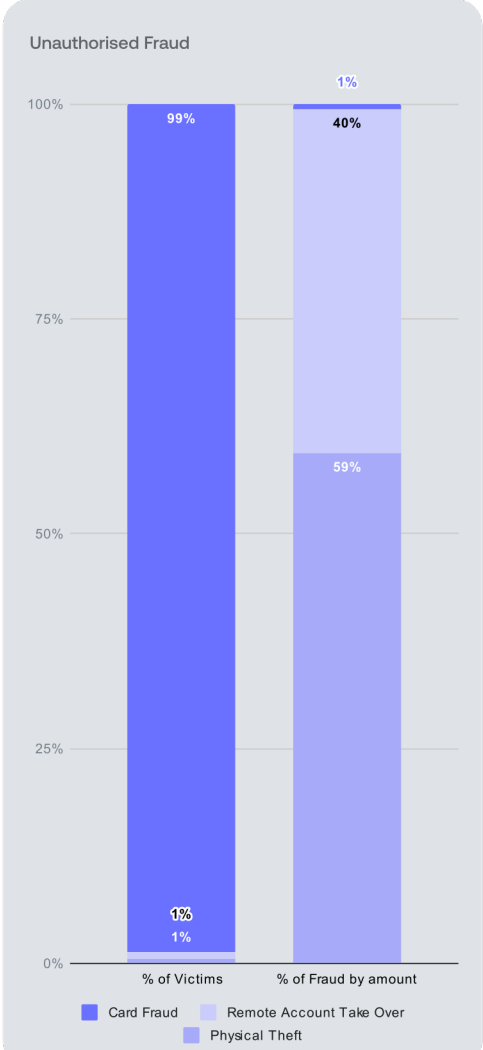
Authorised Fraud

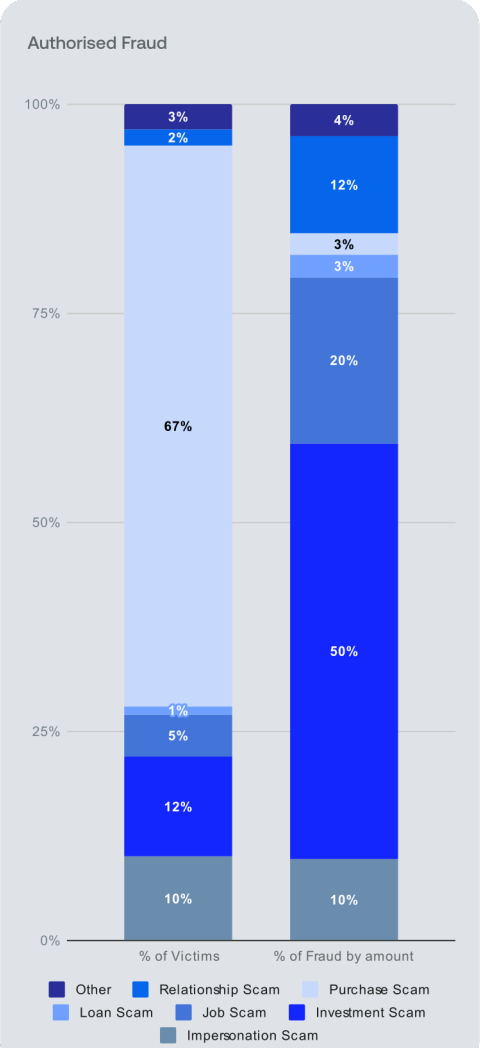


PORTUGAL


Average loss per customer
7%
93%
Authorised fraud
Unauthorised fraud


% of victims by Typology
22%
78%
Authorised fraud
Unauthorised fraud


Unauthorised Fraud
100%
75%
50%
25%
0%
99%
1%
1%
40%
59%
% of Victims
% of Fraud by amount
Card Fraud
Remote Account Take Over
Physical Theft


Authorised Fraud
100%
75%
50%
25%
0%
3%
2%
67%
1%
5%
12%
10%
4%
12%
3%
3%
20%
50%
10%
% of Victims
% of Fraud by amount
Other
Relationship Scam
Purchase Scam
Loan Scam
Job Scam
Investment Scam
Impersonation Scam