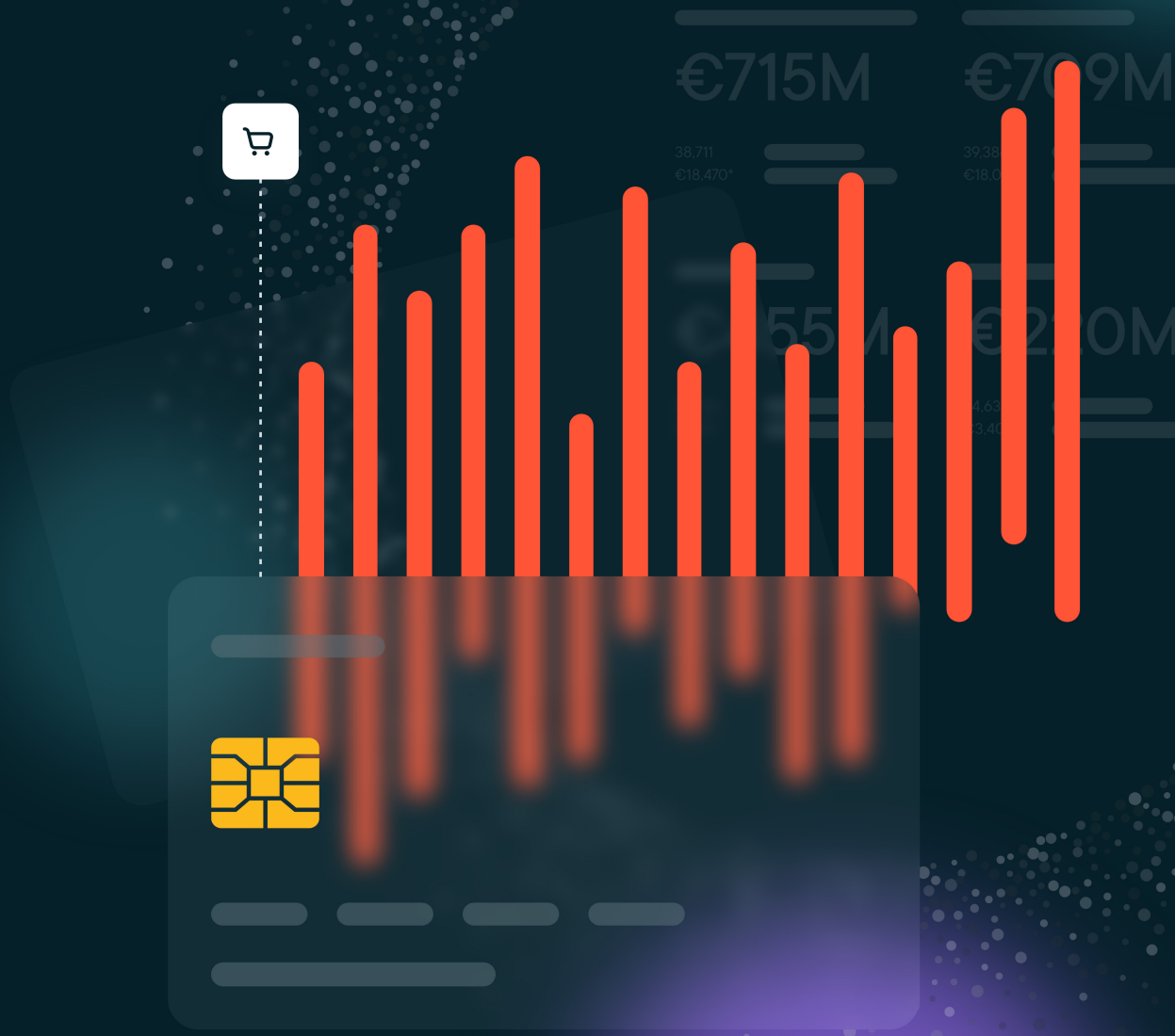
Fraugster

Payment Intelligence Report 2022



Introduction

We are proud to introduce Fraugster's first Payment Intelligence Report, a summary of the most important Compliance, Fraud Risk and Revenue Uplift trends in the market right now.

We have distilled these into discrete sections that can be enjoyed one at a time over a cup of coffee, or read together to form a richer picture of "need to know trends" that should be on your radar.

60B

Data points and

80M

individual transactions analyzed for fresh insights

What you can expect to learn

01: Fraud Tactics

The latest **fraud tactics** being deployed against PSPs, BNPLs and Merchants in Travel, Physical Goods and Digital Goods.

02: Trivia & Surprising Facts

Fun and often **surprising facts, figures and trivia** you can share with your risk management, fraud prevention, payment, compliance and e-commerce network.

03: BNPL: Threats and Challenges

A “Quick Dive” into the **challenges and opportunities for BNPLs**, and why they are experiencing a greater challenge with bad debts than credit card providers.

04: Chargeback trends

A “Quick Dive” into the latest data on **Chargeback trends** and chargeback reason codes.

05: PSD2 impacts

A summary of **PSD2 impacts**, and if 3DS2 is improving or reducing final approval rates for merchants. The situation is different from what you might expect.

06: Fraud Stories

A summary of the **most relevant fraud stories and vectors of attack** that we have been observing across verticals and regions.

07: Future Trends for 2022

A strong point of view on **future trends for 2022 and beyond.**

Enjoy your reading

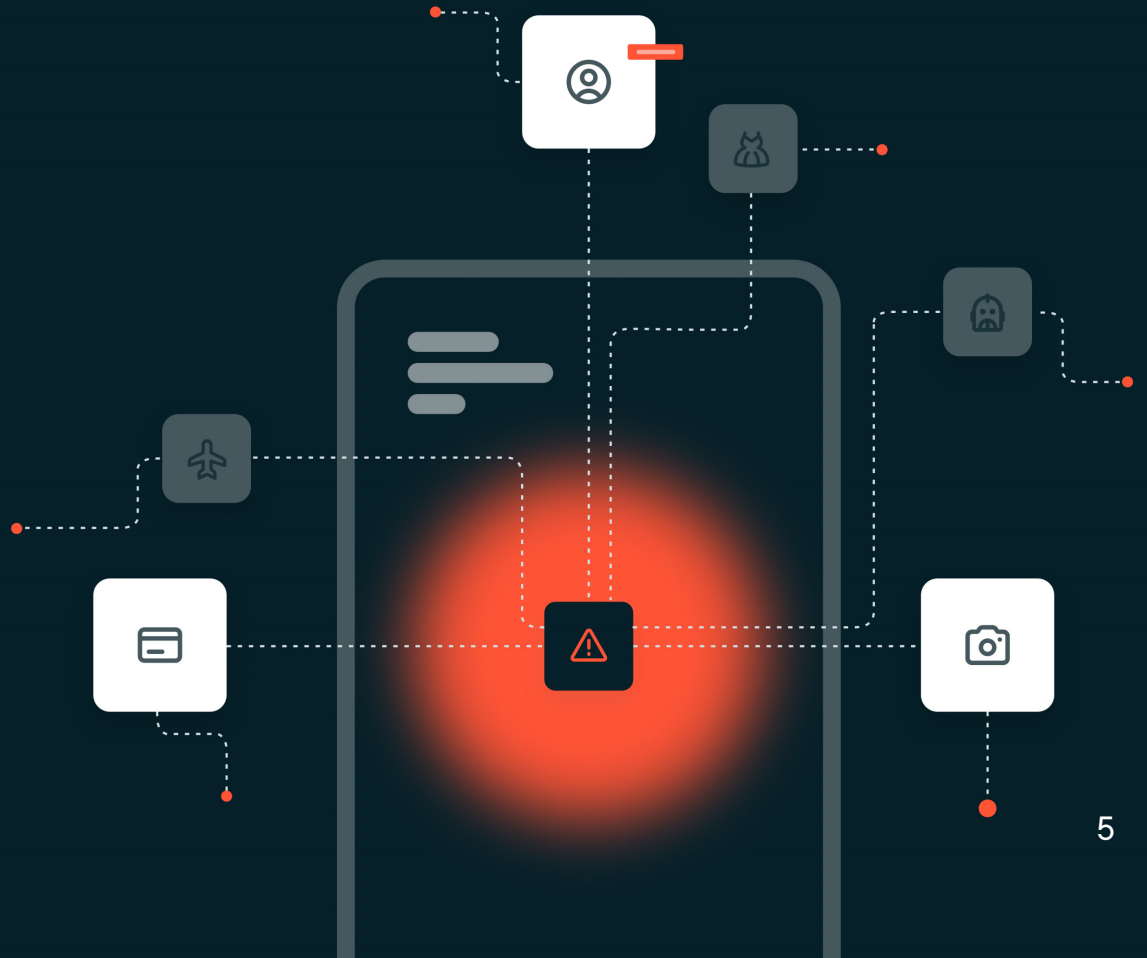
The authors

Max Wolke
Head of Strategy at Fraugster

Aditya Srivastava
Strategy Analyst at Fraugster

Clara Pestalozza
Fraud Analyst at Fraugster
(Supported by: Livia Zambotti, Aleksandra Kwiatkowska)

Part 01
Fraud tactics



The good, the bad, and the surprising

Cost of Personally Identifiable Information (PII) on the dark web

Credit card

Details for credit cards with an account balance up to €5000 — **€223**

The price of a cloned credit card — **€23**

Cost of hacked Israeli credit cards compared to UK and US credit cards which fetch between € 19-23 — **€60**

Passport

Passports issued by tax havens with fewer international extradition treaties, like Malta, command the highest prices on the dark web

€6K

The price range for a passport of an EU member state

€3.7K-5K

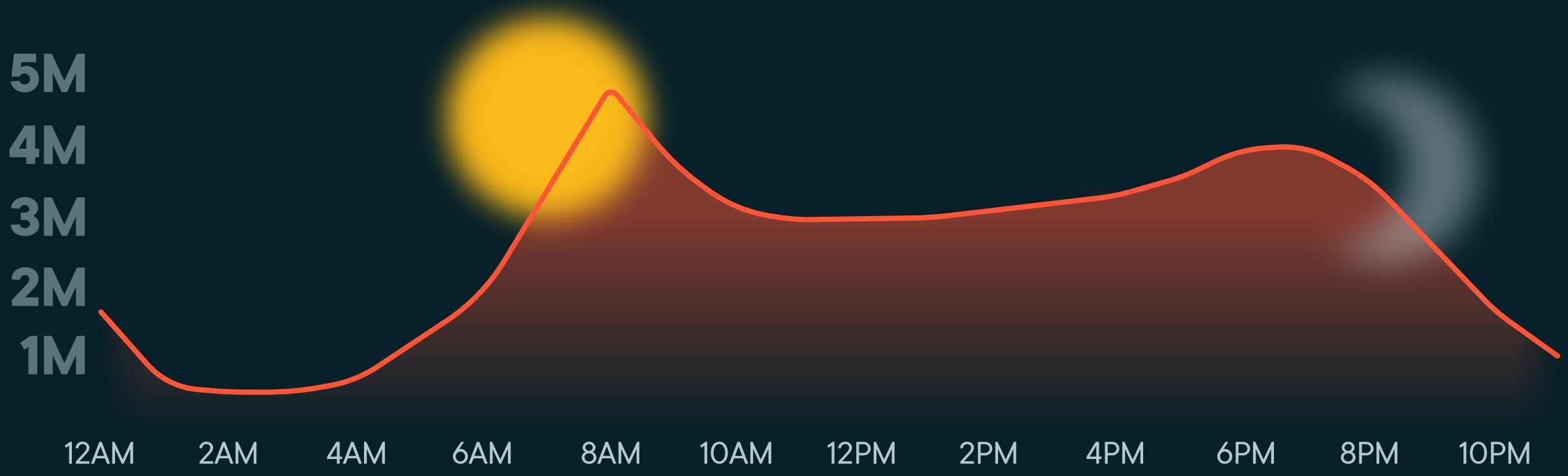
Photo ID

The cost of a selfie whilst holding an ID used for KYC checks costs

€93

Morning retail therapy*

Preferred shopping times based on number of orders at a particular time.



*No. of orders in Millions

Average chargeback value by vertical / Total cost of chargeback 2.9x multiplier

Travel

€710 / €2060

Gaming

€25 / €72

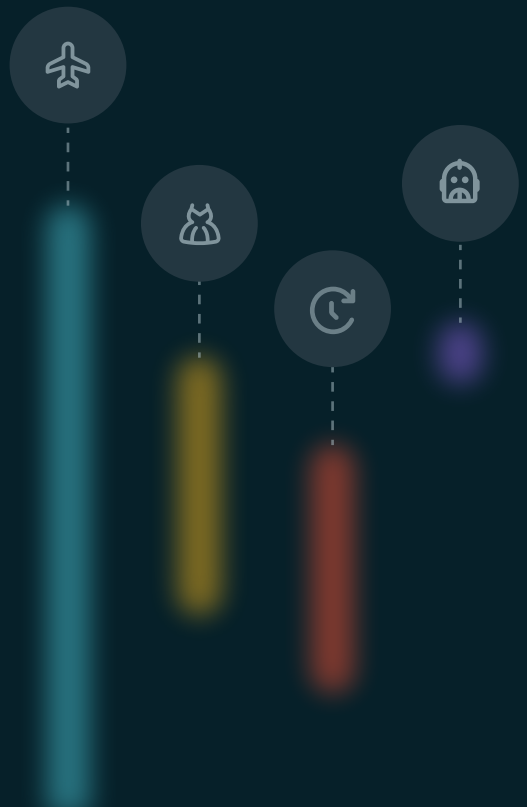
Fashion

€220 / €640

Edtech

€165 / €480

Average order value (AOV) by vertical



€580
Travel

€147
Physical Goods

€146
Buy Now Pay Later (BNPL)

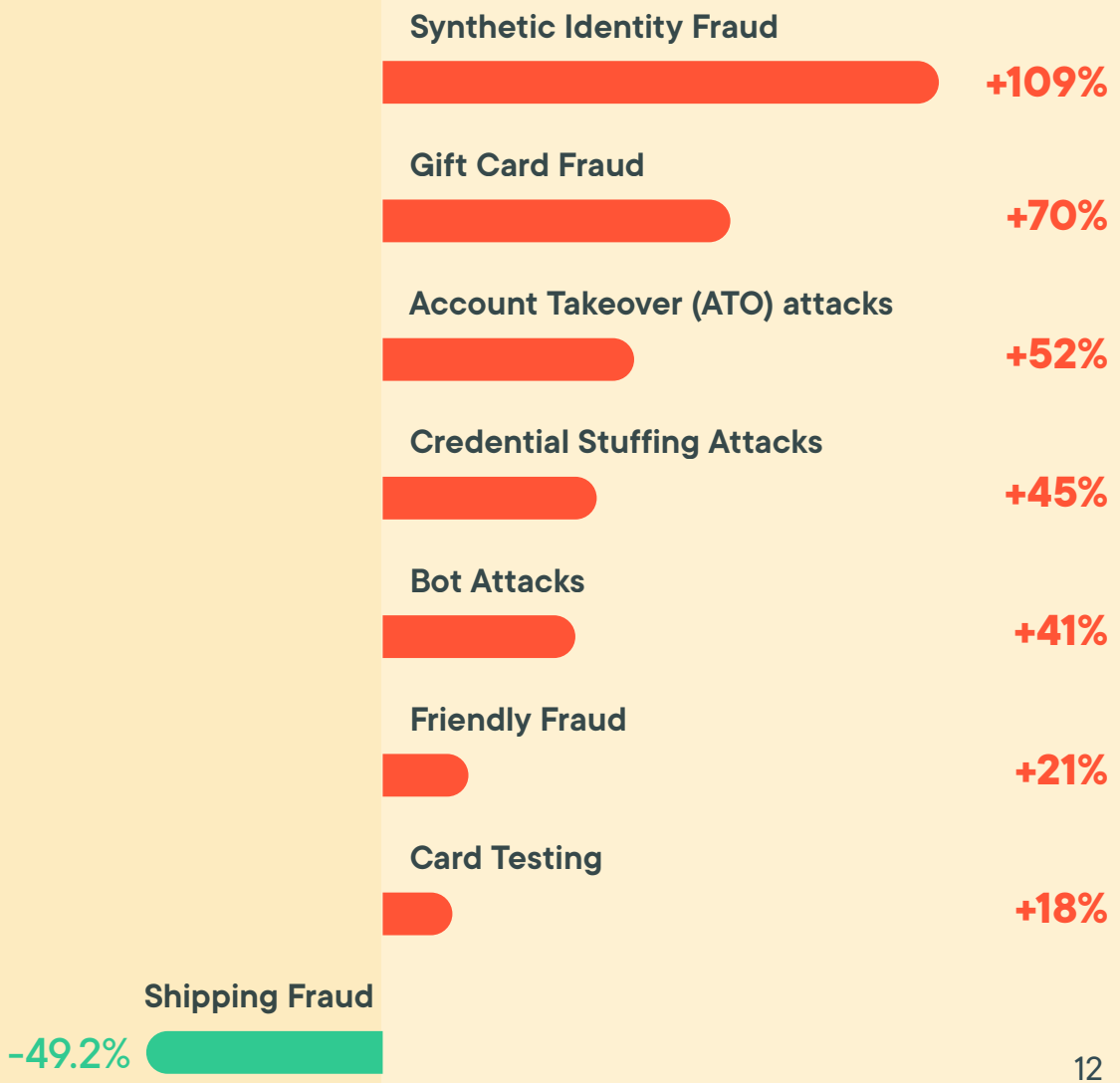
€20
Digital Goods

Part 02

Surprising facts, figures and trivia

Need-to-know payment intelligence trends

Year on year changes (%) by fraud type



+109%

Synthetic Identity Fraud

Where a fake identity is created from stolen credentials (national security, financial instruments, social media footprint etc.) to bypass customer verification protocols.

+70%

Gift Card Fraud

Involves a fraudster purchasing e-gift cards using stolen payment information and then using or reselling them for a profit.

+52%

Account Takeover (ATO) attacks

Involves Fraudsters obtaining legitimate customer credentials, usually as a result of a data breach, to then use these to login and “takeover” an account to order goods.

+45%

Credential Stuffing Attacks

Involves Fraudsters using stolen usernames and passwords from one organization obtained from a data breach or purchased via the Dark Web to access the user accounts of another organization.

+41%

Bot Attacks

Automated web requests used to manipulate and defraud an application, website or an end user.

+21%

Friendly Fraud

Involves a cardholder exploiting chargeback reimbursement policies by filing a chargeback against a merchant without any legitimate reason.

+18%

Card Testing

Where Fraudsters try to determine whether stolen card information is valid before committing larger scale fraud. Multiple low value purchases are made to stay under the radar.
If successful the same payment instrument is used to buy higher value goods and services.

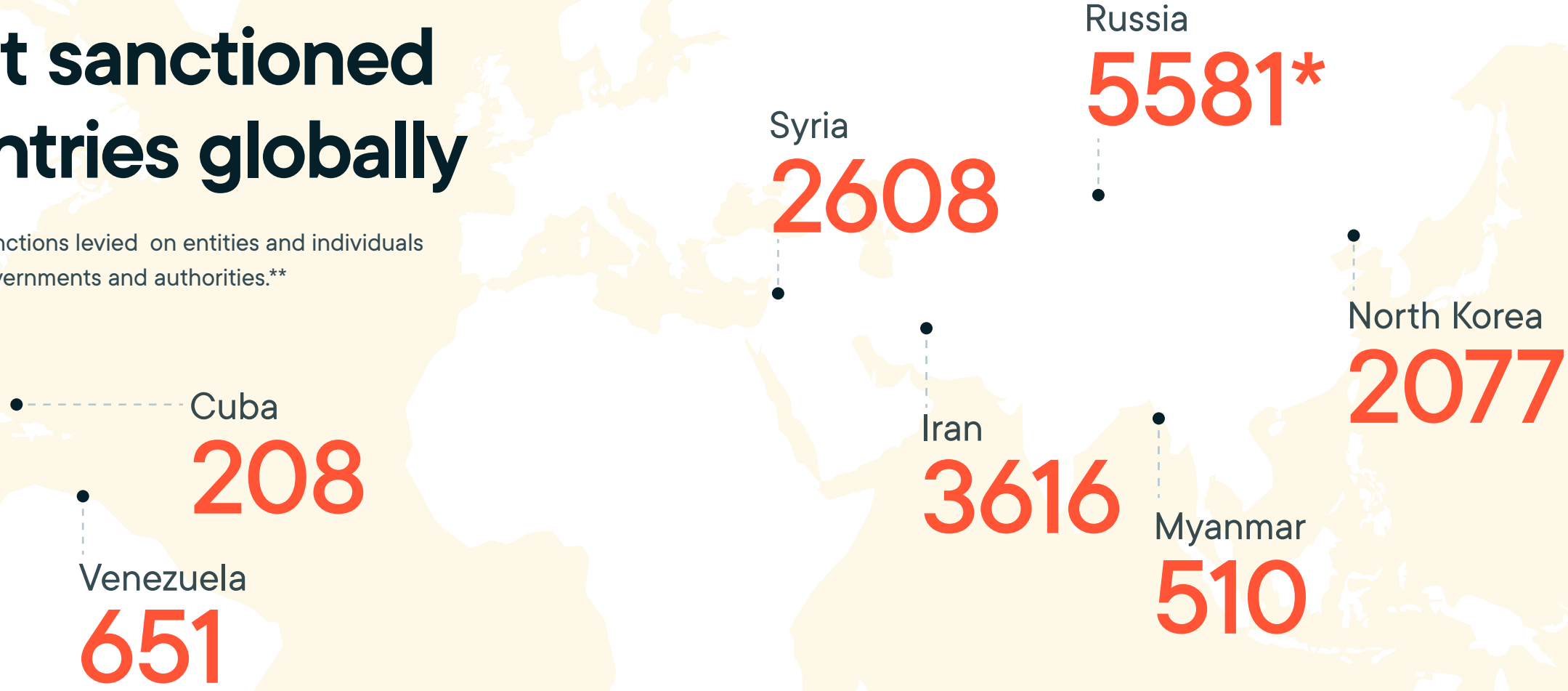
-49.2%

Shipping Fraud

Involves a fake buyer spoofing a shipping address or a seller receiving payment for goods or services, but never shipping it to the buyer.

Most sanctioned countries globally

Number of sanctions levied on entities and individuals by various governments and authorities.**



Source: Statista

* Out of which 2827 have been imposed after Feb 22

** Sanctions by USA, UN, EU, Australia, Canada, India and Israel

A summary of fines for Anti-money laundering (AML), non-compliance

Every year entities and individuals face severe penalties and a loss of reputation due to their failure to comply with Anti-money laundering (AML) standards set by governments in various jurisdictions with an aim of preventing fraud, illicit financing and financial crime.

€2.5B
AML fines in 2021

80
Institutions fined (from just 24 in 2020)

€31.79M
Average fine

€5.6B
Total AML Fines (2015-2021)

Source: Kyckr

What payment methods attracted the most fraud?

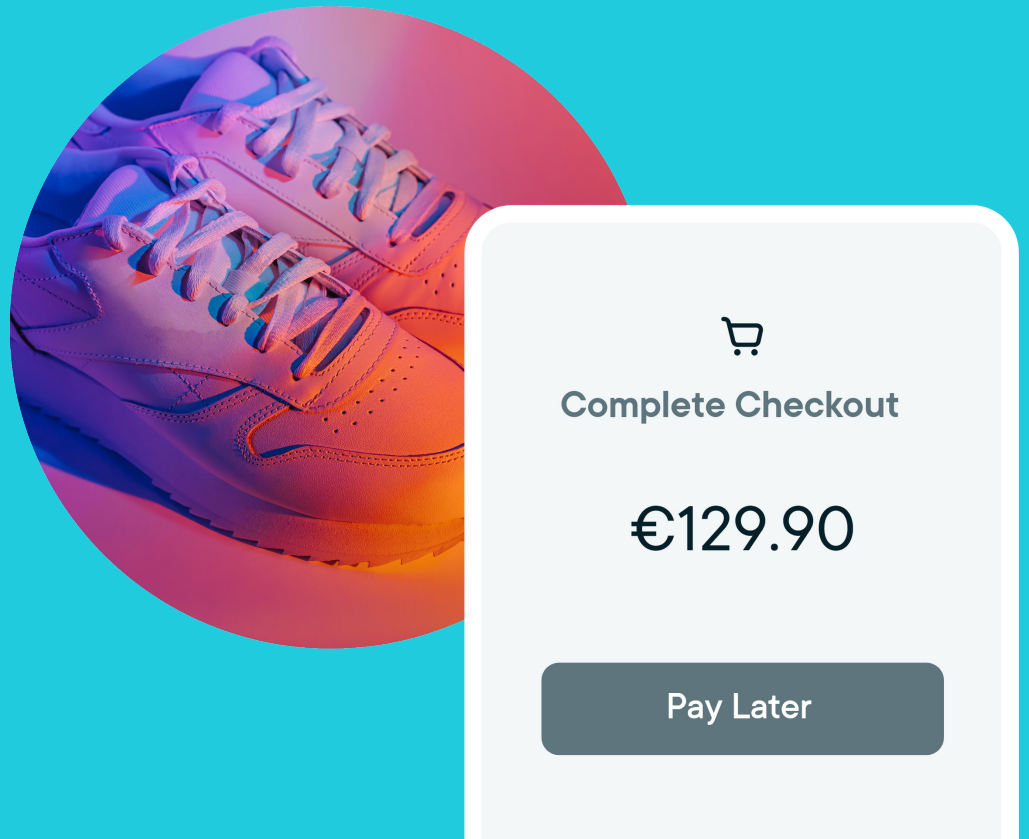
* Data pertaining to the USA; amounts converted from $ to €
** Includes fraud in electronic fund transfer, Automated Clearing house (ACH)

Payment method	Cases	Amount*
Credit Card	88,354	€171M
Debit Card	69,937	€132M
Payment App/Service	69,753	€122M
Gift Card	64,638	€220M
Wire Transfer	58,026	€455M
Cryptocurrency	39,386	€709M
Bank Transfer/Payment	38,711	€715M**

Source: Federal Trade Comission, Consumer Sentinel Network, February 2022

Part 03

Challenges & opportunities for BNPLs



Bad debts as a percentage of outstanding debt: Credit Cards VS Buy Now Pay Later (BNPL)

Bad debt percentage for Credit Cards:

5.30%

(Source: MotleyFool)

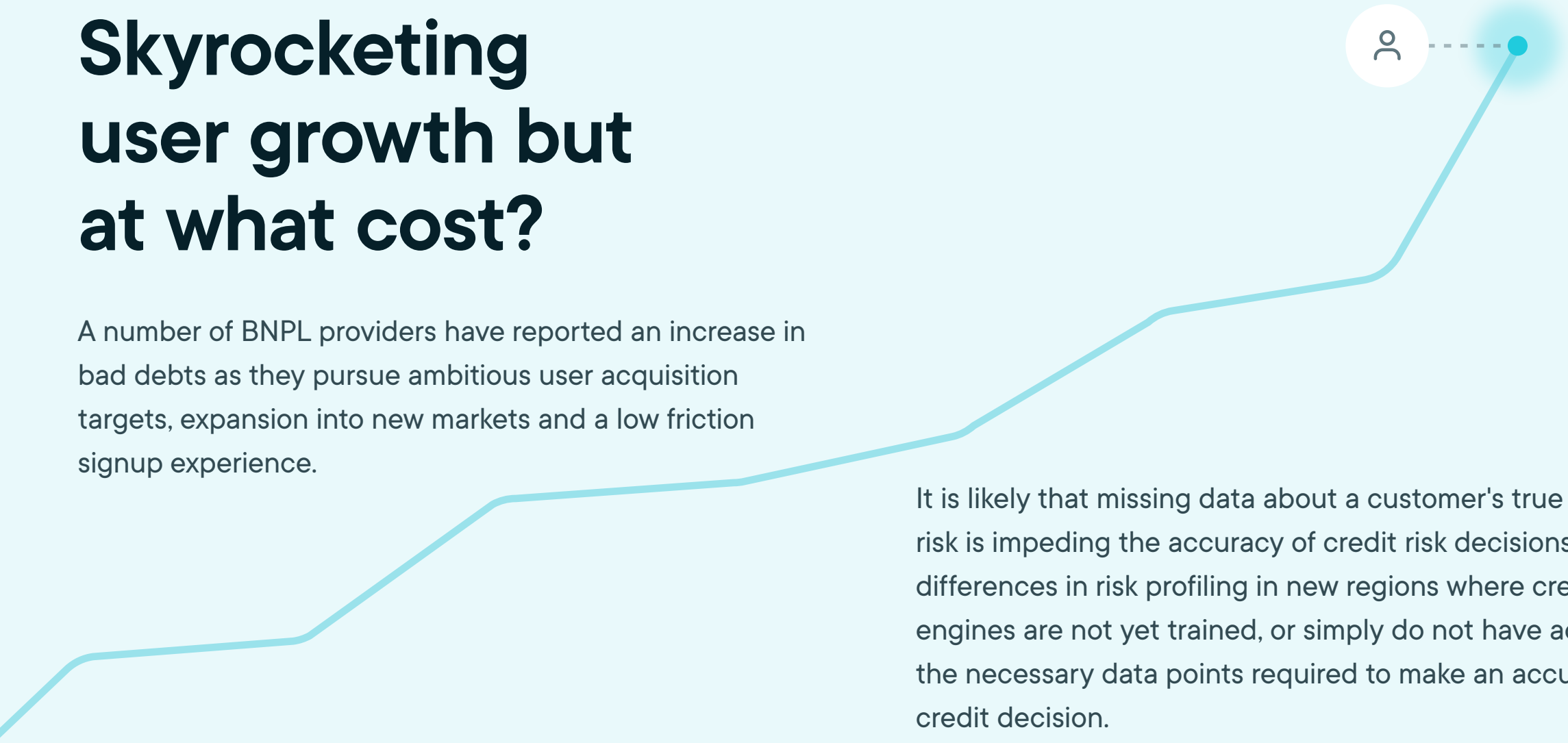
Bad debt percentage for BNPL providers:

9.55%*

* Estimated percentage based on bad debt percentages of top BNPL providers

Skyrocketing user growth but at what cost?

A number of BNPL providers have reported an increase in bad debts as they pursue ambitious user acquisition targets, expansion into new markets and a low friction signup experience.

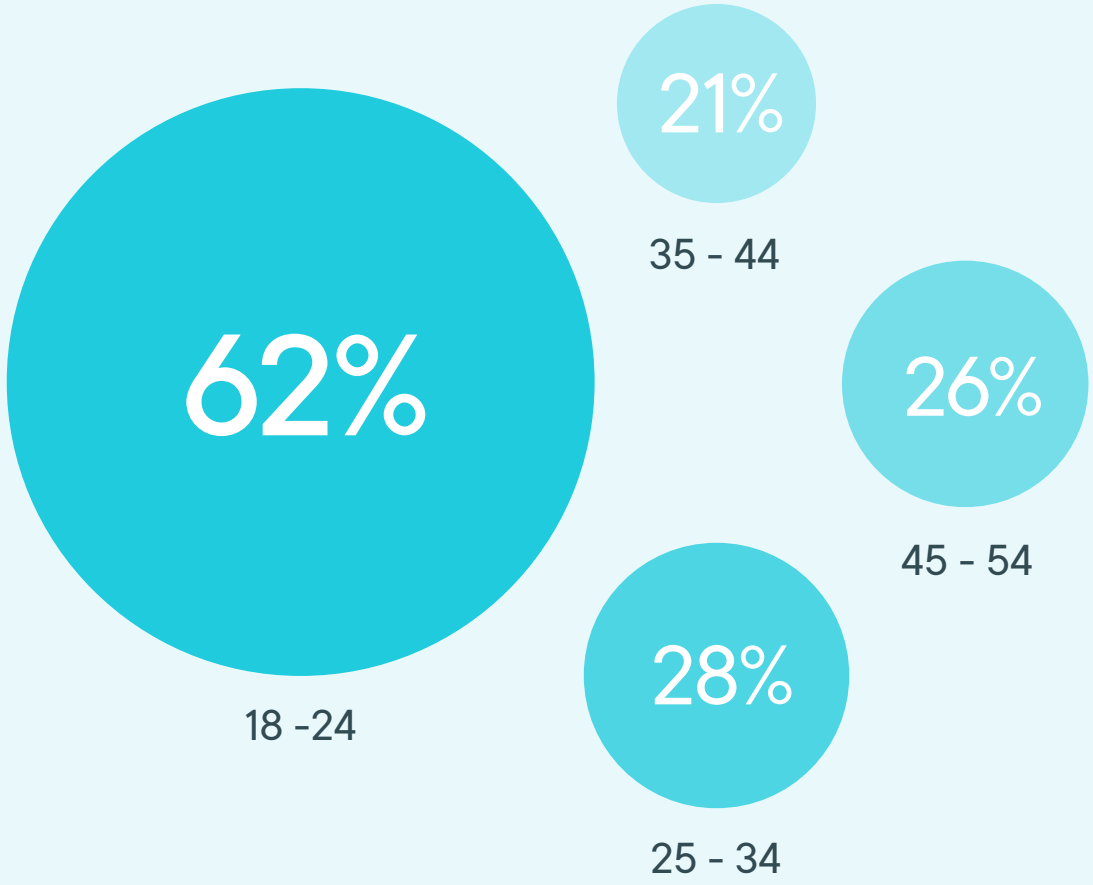


It is likely that missing data about a customer's true credit risk is impeding the accuracy of credit risk decisions, as are differences in risk profiling in new regions where credit risk engines are not yet trained, or simply do not have access to the necessary data points required to make an accurate credit decision.

Skyrocketing user growth but at what cost?

This may be especially true when assessing younger age cohorts in the **18-24 bracket** who have a more limited credit and transaction history compared to older cohorts who may already be using a range of financial products. They grew by a massive **62% YoY** and represented the fastest growing new user group for BNPLs.

BNPL user growth by age

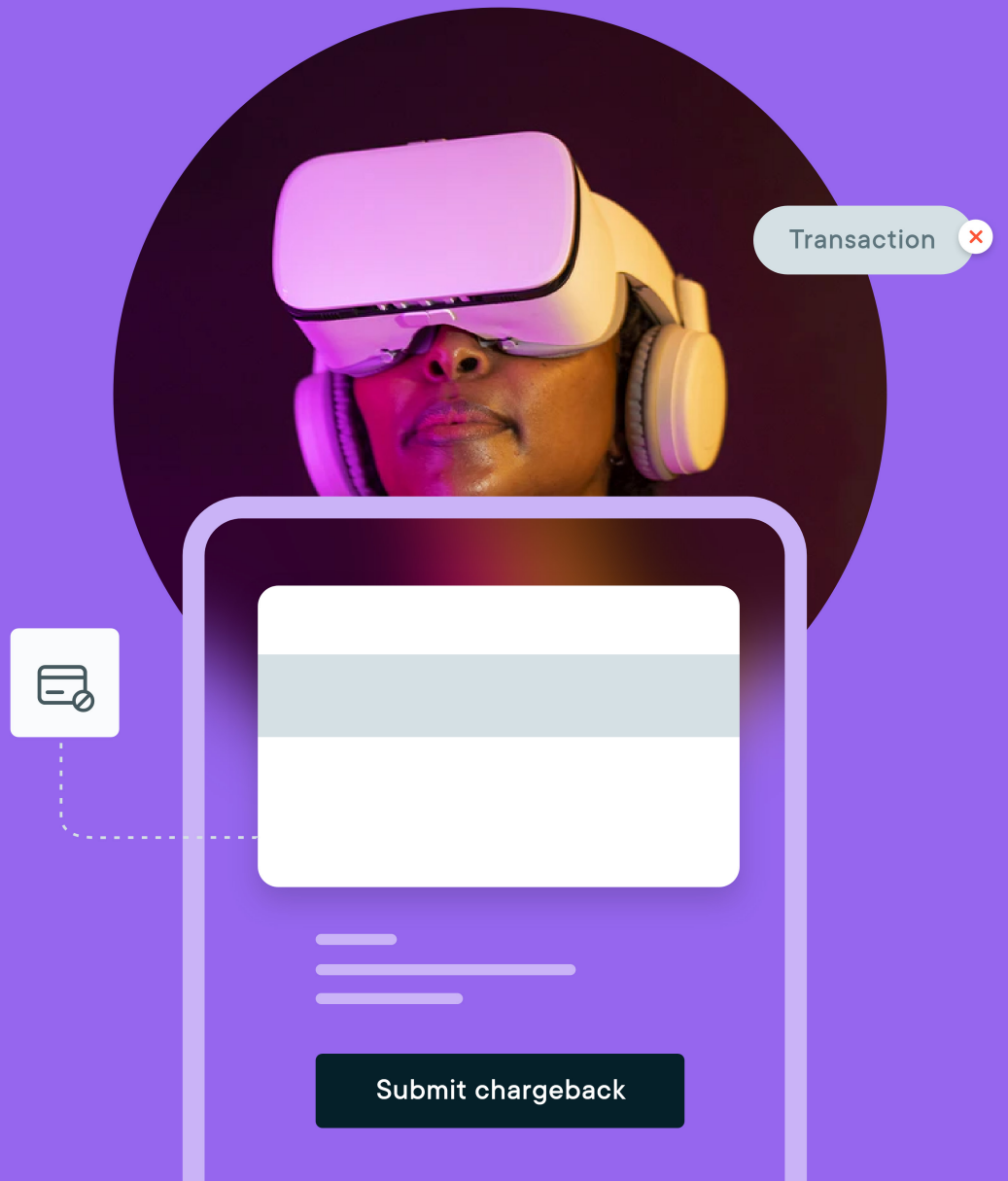


Source: Fool.com

In order to assess risk accurately to avoid bad debts piling up, BNPL solution providers need to look for data sources that go beyond performing traditional credit checks and assessing users' in-app activity.

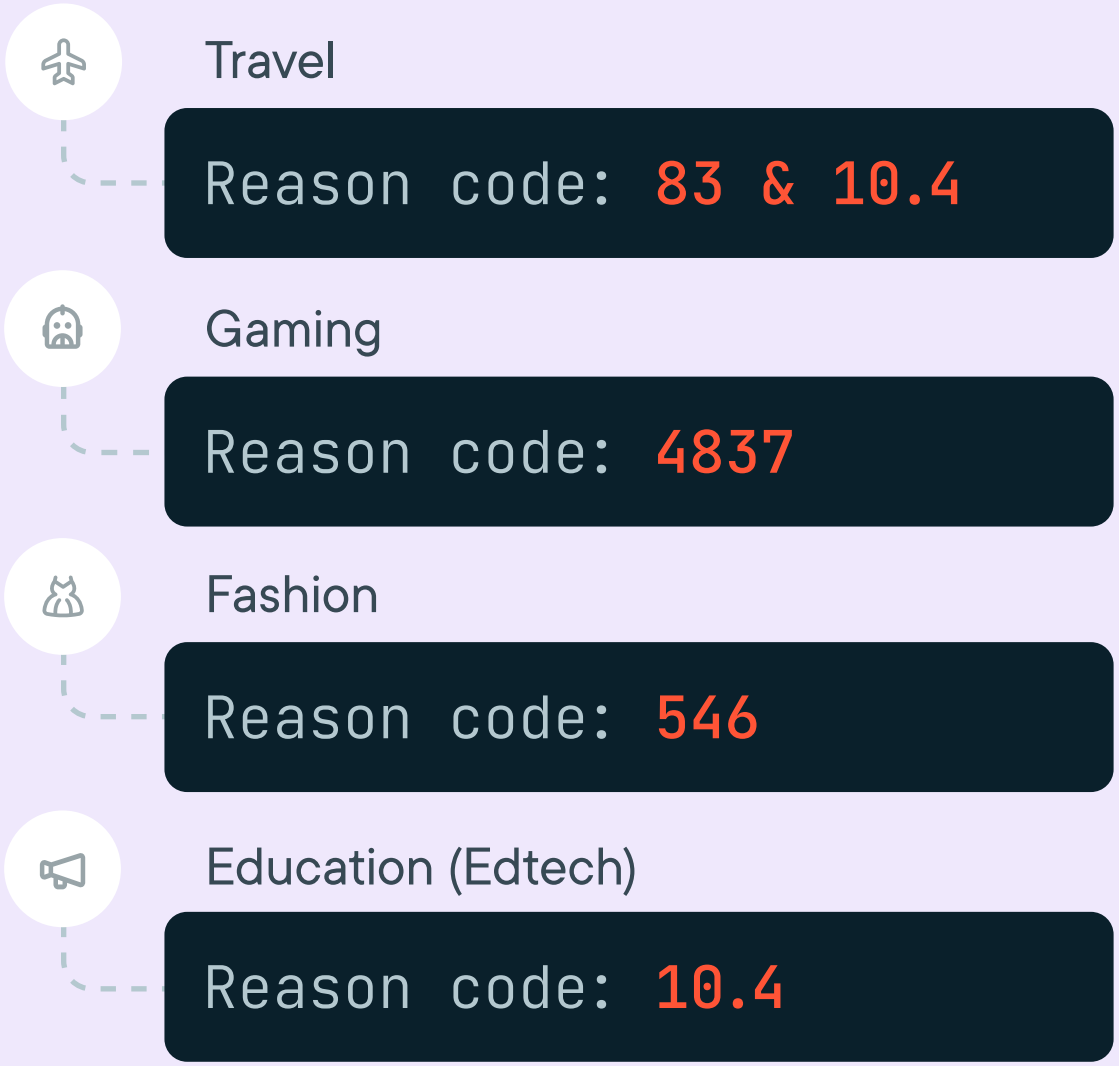
The additional data points Fraugster recommends analyzing to build a more accurate and holistic picture of credit risk are **positive transaction history, unpaid amounts, total spend, device ID and buyer account history.**

Part 04
Chargeback Quick Dive



Common chargeback reason codes by verticals

The following reason codes specified by major card networks pertain to the cardholder not participating or engaging in a **Card Not Present (CNP)** transaction.



46%

of total chargebacks are filed within a

60

day span

A key reason for this is a **120-day limit** set by major card networks (from the date of transaction) for cardholders to file a chargeback.

However, cumbersome procedures set by banks involving multiple forms and calling various bank personnel, make the process drawn-out for cardholders.

On the other hand, fraudulent chargebacks remain to be a key issue for merchants and can cost them **2x** of the transaction amount.

An example from one of our **travel merchants**, who bear the impact of fraudulent chargebacks, given their high order value.

€1,500
Transaction amount

€2,183
Total financial impact of a chargeback

€1,500	€53	€350	€60	€170	€50
Chargeback amount	Lost margin on goods or services	Marketing costs	Processing fee	Operations fee	Prevention alert fee

Case of angry chargebacks

in sectors most impacted by the lockdowns

The pandemic put millions of customers under emotional and financial stress. Those affected by global travel restrictions and mass cancellations were highly impacted.

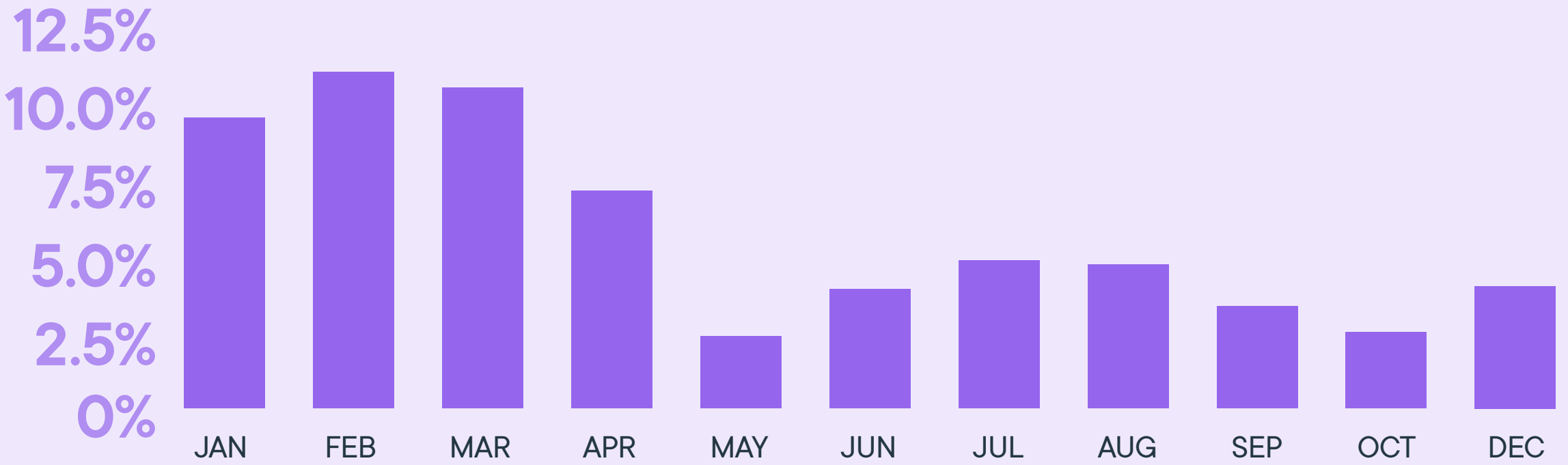
3X

increase in refunds offered by travel merchant in EU and LATAM in

Q1 21

to customers affected by cancellations

Refund % as a proportion of approved transactions



Angry chargebacks increased from

15%

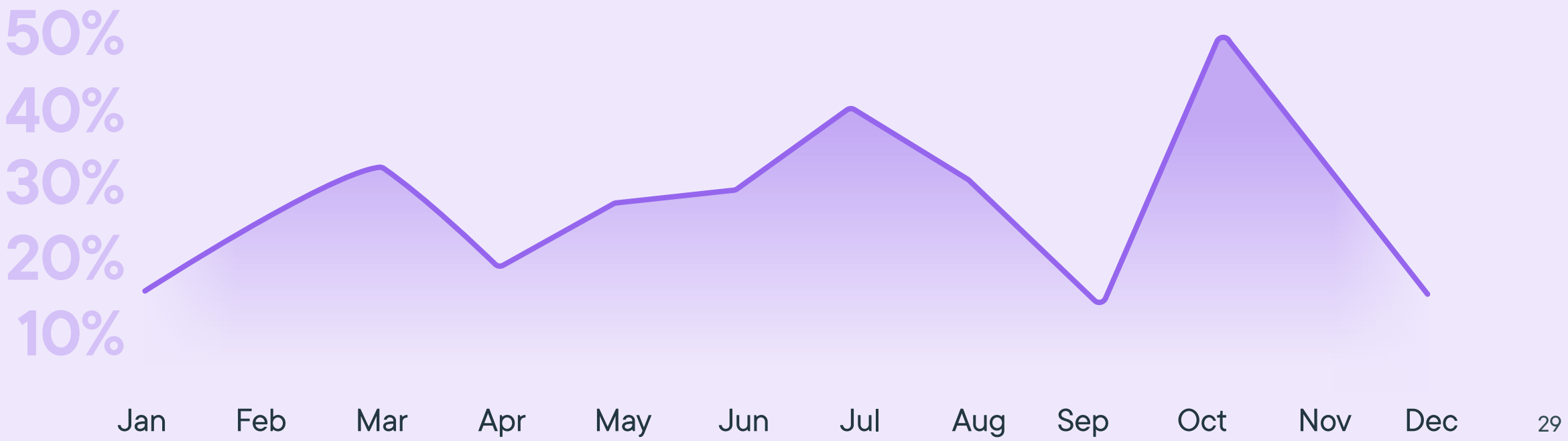
to over

50%

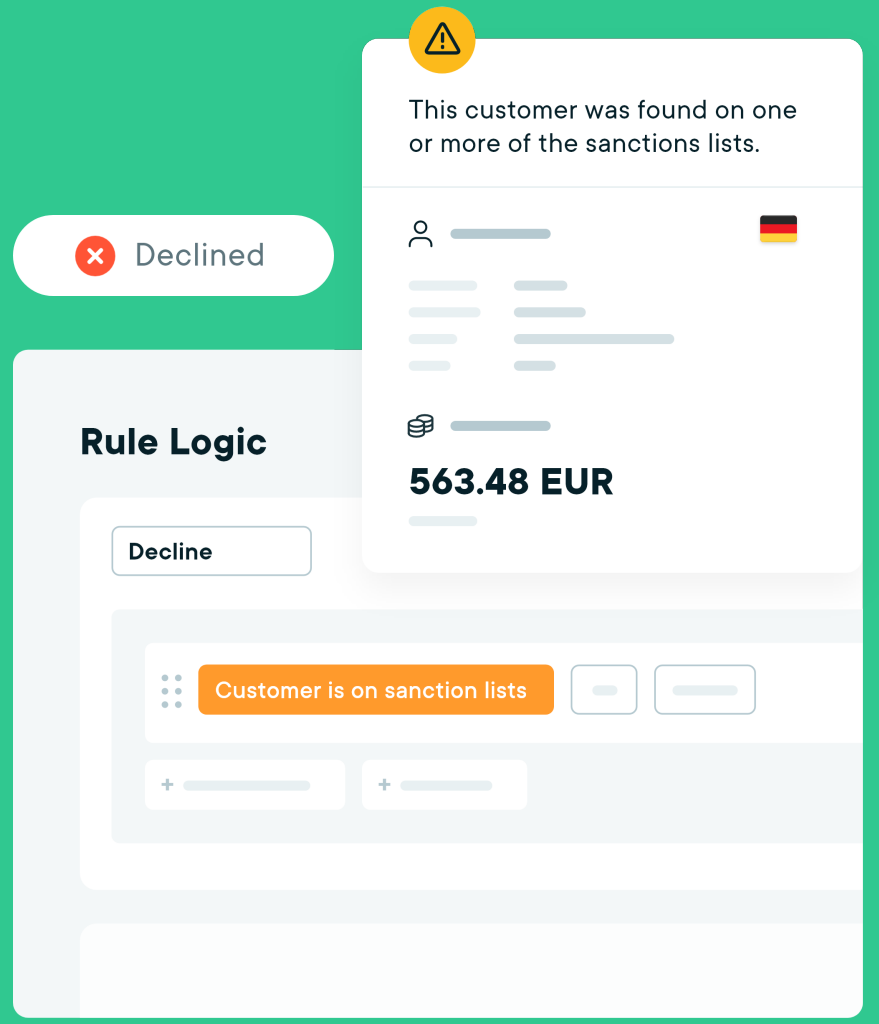
Despite spikes in refunds, a number of customers were left confused and unanswered. As a result of this, customers resorted to using chargebacks as a **revenge tool** while ignoring its financial impact on merchants.

Our data shows a significant increase in angry chargebacks, (defined as chargebacks filed by customers where the merchant is unwilling to offer a refund), increasing from a pre-pandemic baseline of **15% to over 50%** during the peak of regional lockdowns.

Ignoring the financial impact on merchants, it was observed that customers resort to chargebacks as a revenge tool.



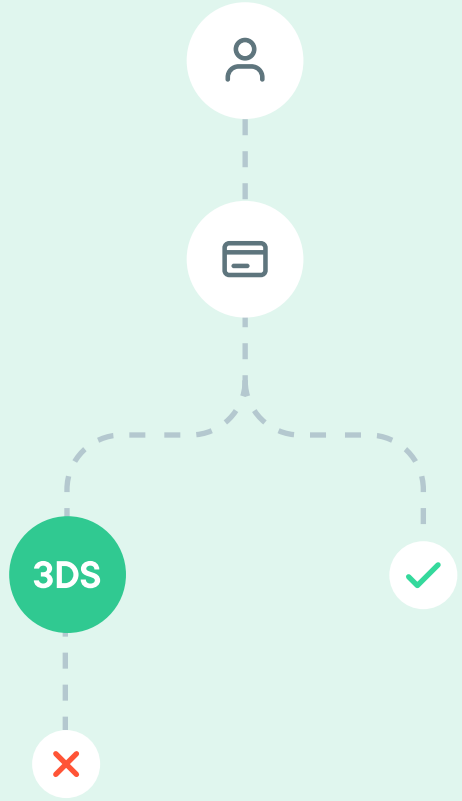
Part 05
Compliance Quick Dive



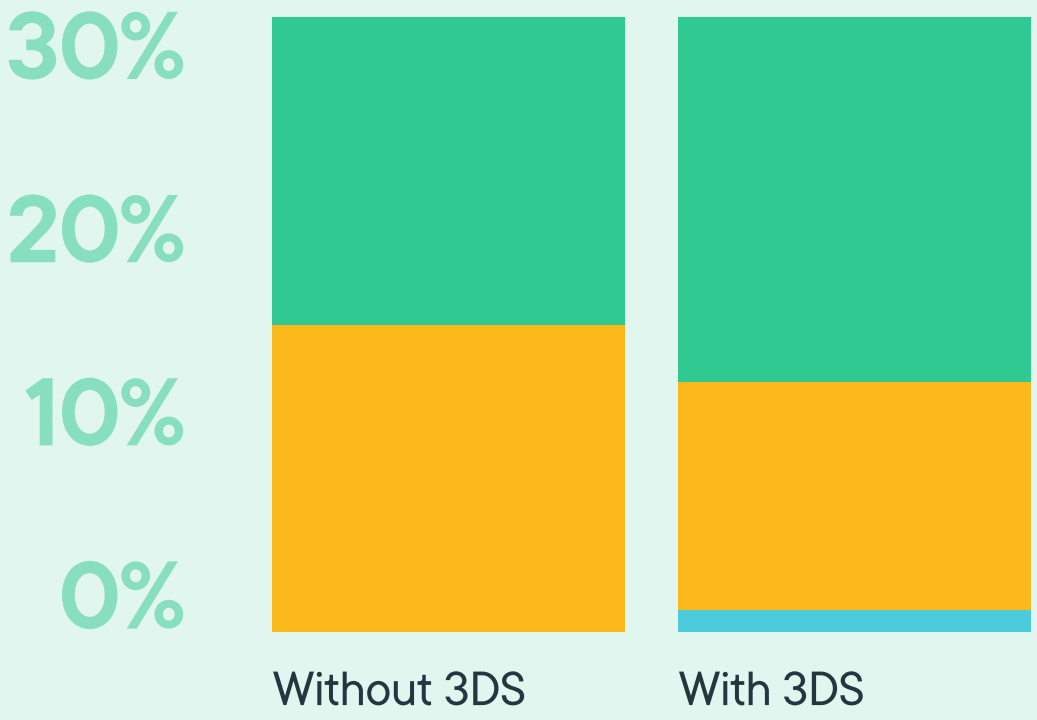
Is 3DS a conversion killer?

The increased probability of customer drop offs has been a major concern for merchants post the introduction of 3DS2.

However, the probability of issuers approving a 3DS approved transaction stands to be more than a non 3DS transaction being approved.



The case of a UK based Issuer



- Authorised
- Issuer bank decline
- 3DS customer drop-off

Here, it can be seen that while there was an increase in customer drop-offs post 3DS, the number of Issuer declines decreases, thus improving or balancing the acceptance rate for the merchant.

As Issuers also gain monetarily by approving more transactions, the majority of them have resorted to directing an increased percentage of their

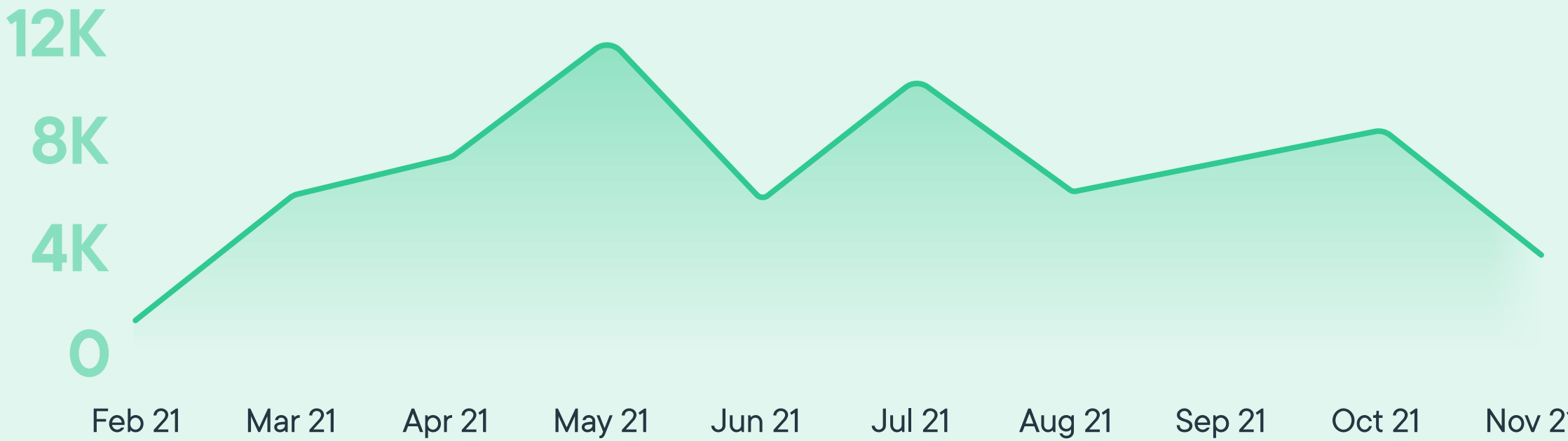
transaction flow, ranging from an estimated

20%-50%

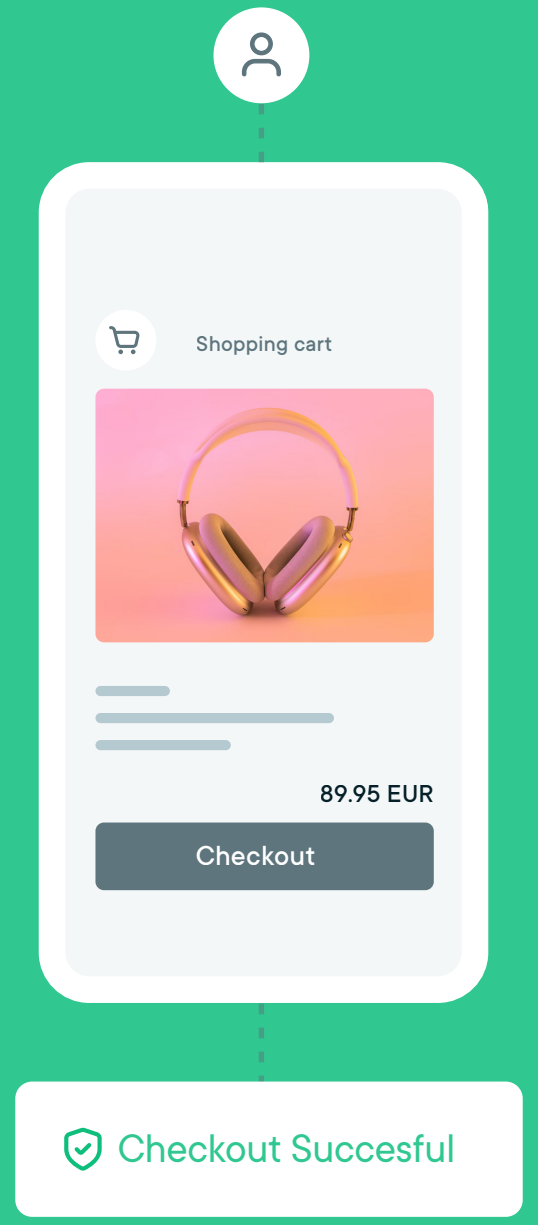
(or even higher for low risk merchants), to **frictionless 3DS** in which the customer would hardly notice the impact of 3DS in their transaction flow.

While merchants can request a 3DS exemption based on transaction risk analysis or the transaction being low value, they cannot solely rely on this to avoid dropoffs.
Our data further points to the volatility in the number of transactions receiving such an exemption.

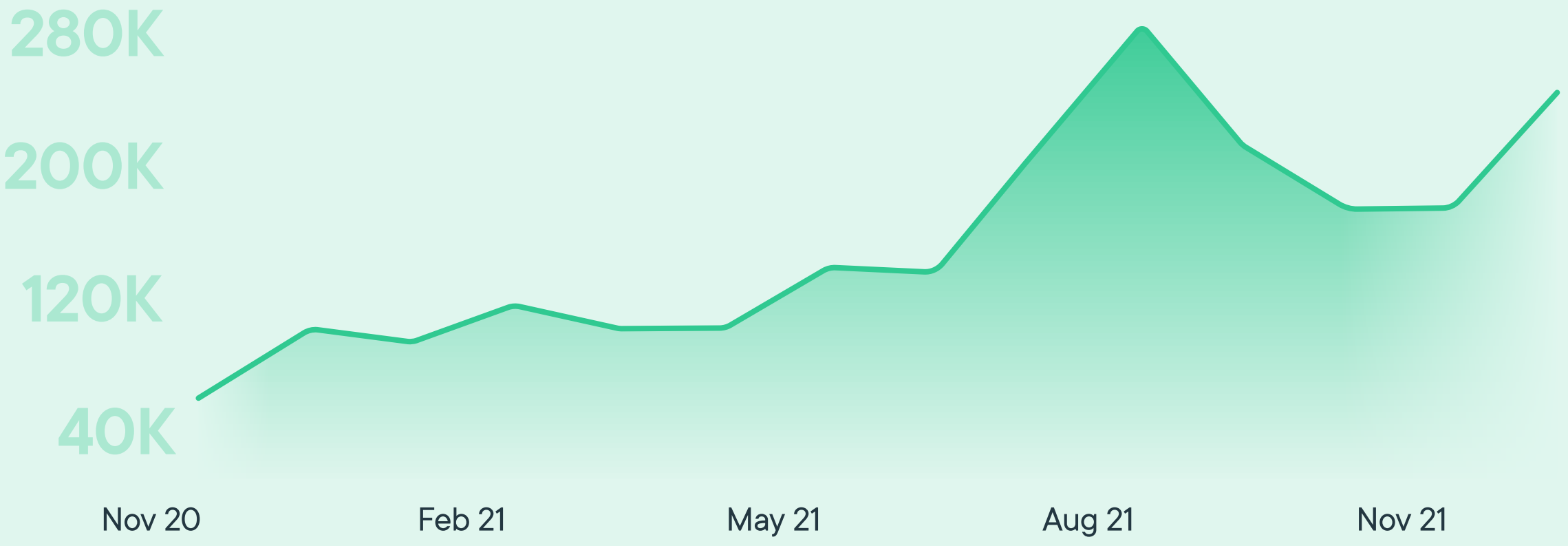
Transactions receiving an exemption from 3DS



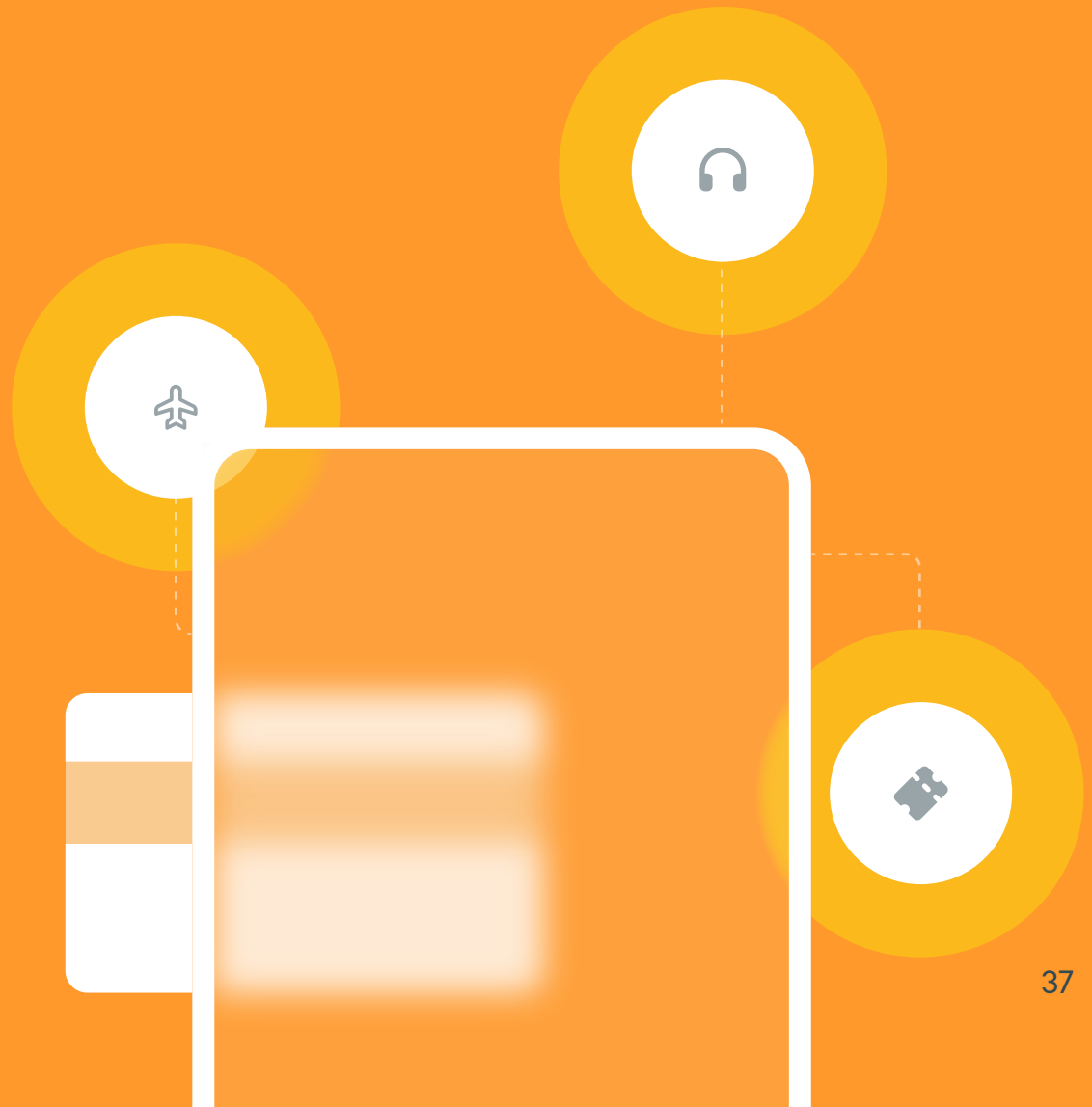
Frictionless authentication aids in providing the customer a seamless transaction journey and reduces the number of dropoffs for the merchant. Given this scenario, it has been noted that the number of fully 3DS authenticated transactions has increased from its date of initiation.



Increase in fully 3DS approved transactions



Part 06
Verticals Quick Dive



Airlines key data

€6.5B+

Lost to fraud in 2021

=24K

Flight tickets

1.5%

of Global Airline revenue lost to fraud in 2021.

€4.5B+

Lost due to legitimate transactions was wrongly identified as fraud (false positives).

15-20%

of all airline bookings are still subject to manual review, costing airlines millions per annum in operational costs.

Airlines fraud stories

Rebooking fraud

Fraudsters use stolen financial information to buy expensive tickets and then resell them again as cheaper “last minute” offers to an unwitting customer via a fraudulent OTA at a competitive price. These expensive tickets are booked well in advance to avoid suspicion.

Airlines are hit with a chargeback when the owner of the stolen credit card notices a transaction they did not make (**most commonly chargeback codes 10.4 or 4837**). The defrauded customer in many cases will be unable to board the flight and blame the airline operator.

Airlines fraud stories

Hostile card fraud

A fraudster buys a flight ticket from London Heathrow to New York (JKF) at the departing airport from their mobile device, using a stolen credit card registered in Asia and a newly created email address. The airline not only loses revenue, but receives a chargeback 30 days later from the customer whose payment details were stolen.

The purchase is made three hours before the flight departure. The short time between the purchase and departure means the Issuing bank is unable to provide a notification to the airline that this is a fraudulent transaction, meaning the booking cannot be canceled and the fraudster cannot be prevented from boarding the flight.

Digital goods key data

€3.85B

Total direct fraud losses for digital goods in 2021 (consisting of gaming, gambling and gift cards).

€13.8B

Worth of genuine transactions lost due to false positives.

4x

False positives amounted to total fraud losses.

32.6%

Highest uptick in fraud for gaming while fraud in the gambling industry increased by 29.4% (mostly identity fraud).

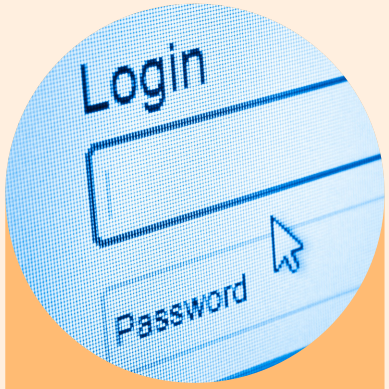
Digital goods fraud stories

Buying gift cards with stolen credit cards

Fraudsters use stolen credit card numbers to buy gift cards online, then either use them to redeem goods or services or resell them. Merchants get hit with a **chargeback** when persons whose credit card details have been stolen find out. This is one of the easiest ways for fraudsters to make a quick win with relatively little effort, and is made even easier for low value transactions, which are subject to **TRA exemptions under PSD2**, meaning no further authentication steps are required.

Digital goods fraud stories

ATO credential stuffing



Fraudsters use stolen logins, often harvested from data breaches to capture customer details like credit card numbers, name, address and email.

These can be obtained as lists relatively easily and cheaply on the **Dark Web**. The fraudster then submits millions of login attempts running through the lists they have obtained, until they get a successful hit. They then go on a buying spree having successfully taken over a customer account (ATO).

Physical goods key data

€4.64T

Generated revenue in 2021 for online sales of physical goods.

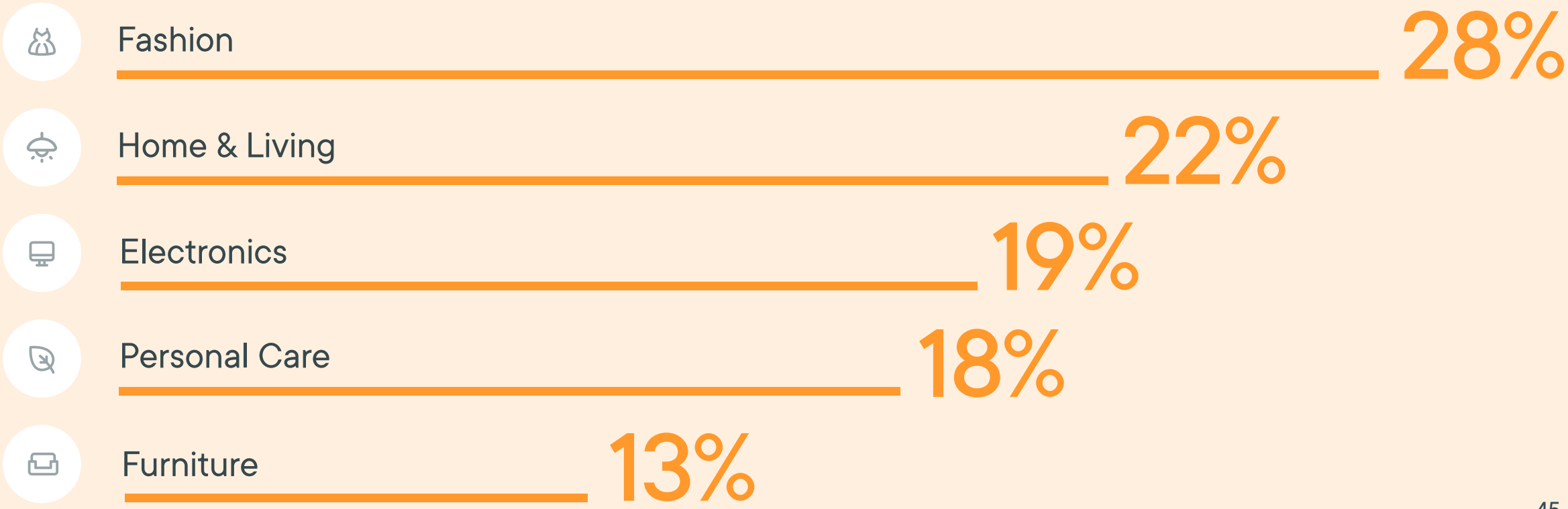
~€69.6B

From the total revenue was lost to fraud in 2021.

1.5%

of total revenue lost to fraud.

Contribution to revenue by %



Physical goods fraud stories

Bot enabled reseller fraud

Electronic goods retailers and sportswear brands often run sales promotions where resellers use BOTs to buy up products in large quantities and then resell them at a premium.

Current mitigations require a great deal of manual effort in customer service to identify and cancel identify and cancel sales that have been allowed through.

A better approach is to detect any **anomalies in buyer behavior** through the matching a large number of attributes.

For example, resellers would be informed about velocity (the number of requests over a certain period of time) via attributes like **Device ID, IP, email, shopping basket contents** and number of goods in the basket.
The preferred payment method chosen might also be an indicator with resellers having a preference for bank transfers which look less suspicious.

Physical goods fraud stories

Rerouting fraud

The fraudster contacts the merchant directly after recieving a confirmation email sent to a fake email address, and changes the delivery to either pickup in store or to an anonymous packstation (a preferred method).

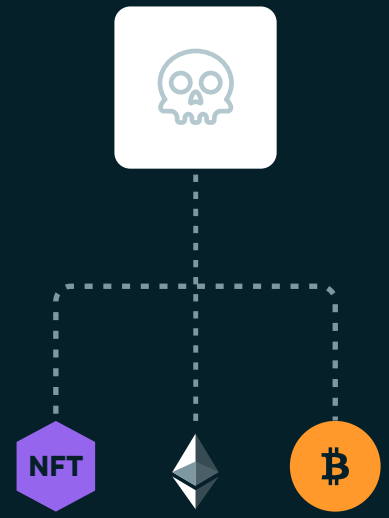
Increasingly fraudsters are bypassing merchants and are contacting courier services directly to change the shipping address, and often this information is not automatically synced with the merchant. This means that even a manual review might miss fraudulent activity. For example, a purchase made with a credit card may show a match between the AVS, billing and shipping addresses.

Part 07

Future Trends

Prediction #01

Fraudsters will exploit the openness of Web3 using stolen financials



The metaverse, also referred to as Web3, is a decentralized version of the internet where platforms and apps are built and owned by users. Meta (previously Facebook), Microsoft, and a host of large gaming companies are the first movers in this space and are building the future of our digital economy.

So, while we should definitely expect exponential growth of digital assets in 2022, this doesn't just mean high value NFTs (Non-fungible tokens), but also low value, high frequency in game purchases for things like swords, skins, and usernames, also known as downloadable content (DLCs).

The main risk this presents is that these environments are preferred locations for fraudsters testing stolen financial instruments (to see if they are approved) before going on to make higher value purchases. This presents a massive chargeback risk for merchants, and especially gaming companies.

Alternative payment methods like cryptocurrencies are not risk free either, as they provide little to no purchase protection to customers. We therefore forecast an increase in fraudsters exploiting the openness of a nascent Web3 using stolen financials that are easily available on the Dark Web, but will soon be even more easily exchangeable in the metaverse.

In parallel we expect to see an increase in the number and value of scams coming from fraudsters masquerading as creators.

A reference example from 2021 was Squid Coin, a fraudulent cryptocurrency named after the wildly popular Netflix series, Squid Games that netted scammers an estimated

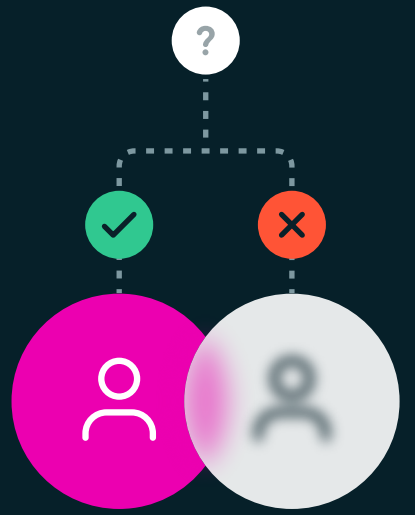
$3.5M

Curators of Web3 environments will need to introduce additional Know your Customer (KYC) checks and better ‘creator monitoring’ to combat this threat. We are already seeing online marketplaces tackling this issue with merchant monitoring solutions, which led us to believe Web3 platforms will need to take similar steps.

The challenge is that Web3 is going to look a lot like the wild west for the foreseeable future, especially as metaverse environments become more interoperable. Therefore consumers will need to be diligent.

Prediction #02

Fraudsters and good customers will become harder to tell apart



More online shoppers are now using VPNs to mask their IP address and protect their personal data online – a behavior that is often seen from fraudsters and that typically increases the risk score of a transaction. Spotting the difference between the two will become more challenging, especially as fraudsters are becoming more sophisticated at mimicking the behavior of good users to avoid detection.

On the one hand this could increase the percentage of false positives, on the other hand it will test how accurately vendor solutions can distinguish good transactions from bad ones, something that can be measured by tracking the Good User Approval Rate.

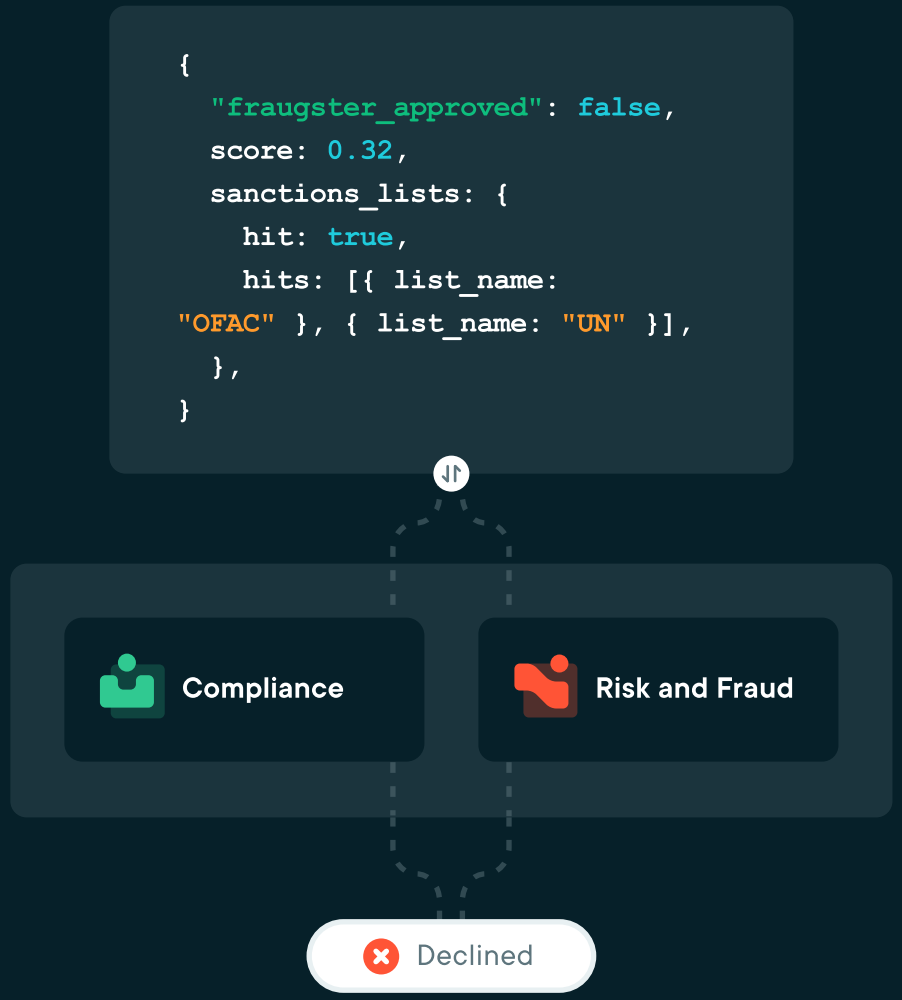
Prediction #03

Compliance costs will continue to spiral, including fines levied against institutions that fall short

2021 saw record fines levied against companies that failed to comply with anti-money laundering regulations. We predict that both total compliance costs (headcount, processing, and vendor costs) and fines levied will increase in 2022.

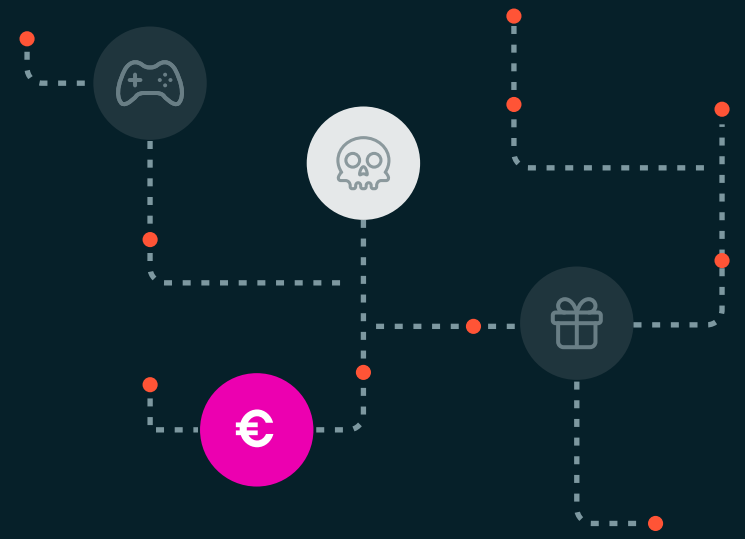
Why? Because the **6th Anti-Money Laundering Directorate (6AMLD)** broadens the scope of money laundering offenses to include those aiding and abetting, inciting and attempting an offense.
This will make it easier for law enforcement to pursue those often described as enablers facilitating money laundering or serving as accomplices in money laundering schemes.

The biggest winners will be those who can leverage technology like transaction monitoring and sanctions and Politically Exposed Persons (PEP) lists to avoid entering into illegal business relationships.



Prediction #04

A fightback against fake identities



In 2021, we saw a massive rise in the use of fake and synthetic identities, constructed from stolen information widely available on the Dark Web. This has made it easier for fraudsters to pass KYC checks for new services like BNPL, gift cards, and online gaming platforms.

We expect this trend to continue, however we forecast a fightback as machine learning algorithms get better at identifying signals that point to an increased probability of fraud, for example a frequent change in IP address, device ID mismatches, and frequent asset hopping.

Make smarter decisions at scale.

Fraugster

Turn fraud prevention into a growth engine.
Start approving more transactions today.
Book a demo

sales@fraugster.com