

# Fraud Prevention in Ecommerce Report 2022-2023

What It Takes to Build Trust and Safety in Digital Commerce



Supporting partners:



Key media partner:



# Fraud Prevention in Ecommerce Report 2022-2023

What It Takes to Build Trust and Safety in Digital Commerce

## Contact us

For inquiries on editorial opportunities please contact:

Email: [editor@thepayers.com](mailto:editor@thepayers.com)

To subscribe to our newsletters, click [here](#)

For general advertising information, contact:

Mihaela Mihaila

Email: [mihaela@thepayers.com](mailto:mihaela@thepayers.com)



RELEASE VERSION 1.0

DECEMBER 2022

COPYRIGHT © THE PAYPERS BV

DESIGN: MYRIAD DESIGN

ALL RIGHTS RESERVED

TEL: +31 20 893 4315

FAX: +31 20 658 0671

MAIL: [EDITOR@THEPAYPERS.COM](mailto:EDITOR@THEPAYPERS.COM)

# Foreword



**Irina Ionescu**

*Content Editor*

The Paypers



Dear reader,

As ecommerce continues to gain momentum in a post-pandemic world, millions of online merchants are fighting a rising phenomenon – *ecommerce fraud*. Ecommerce fraud happens when scammers intercept a commercial transaction at an online store, aiming to gain a personal or financial benefit.

With the 2022-2023 edition of our *Fraud Prevention in Ecommerce Report*, we are looking at **how the fraud ecosystem evolved**, so that merchants and businesses can be one step ahead of the game and deploy effective security methods to win the battle against fraudsters. In addition, we will delve into the latest fraud prevention strategies involving AI, machine learning, behavioural analytics, biometrics, and reliable authentication tools that **help organisations provide a safe environment in online payments** both for them and their end-clients.

## Context and the size of the market

With global **ecommerce sales expected to reach USD 5.5 trillion by the end of 2022**, fraudsters have plenty of opportunities to hijack customer data and commit fraud.

According to the MRC report on Global Payments & Fraud, phishing/pharming, identity theft, and first-party misuse remain the most prevalent types of fraud attacks, affecting almost four in ten merchants globally. Moreover, payment fraud cost ecommerce merchants 3.6% of their total revenues in 2022, proving fraudsters are not only here to stay – but they continuously improve their techniques and technology to create new ways and perfect the old scamming schemes.

Between 2021 and 2025, **merchants stand to lose up to USD 206 billion on fraud**, with remote physical goods purchases being the leading cause of online payment fraud, accounting for over 47% of all fraud losses in 2021. At the same time, fraud detection and prevention platform services are set to exceed USD 11.8 billion globally in 2025, a significant increase from the USD 9.3 billion figure in 2021.

As more consumers expect greater speed, flexibility, and convenience in the way they pay, the new shopping habits (e.g., digital gift cards, BNPL) opened doors for fraud attacks: whether new forms of fraud are emerging (e.g., Fraud-as-a-Service, account reactivation) or old types of fraud (e.g., ATO, chargeback fraud, synthetic identity fraud) are becoming more sophisticated, fraudsters don't miss the opportunity to explore any loopholes.

At the same time, the current global economic downturn – caused by the *ongoing war in Ukraine and spikes in prices of gas and energy* – which led to an increased inflation rate and a potential new worldwide recession also impacted the fraud sector, as scammers are eager to prey on the weak ones. →

# Foreword

With the end of 2022 right around the corner and all these challenges ahead, we invite you to follow the narrative line of our industry experts – associates, consultants, and merchants –, as we dive deeper into the world of fraud prevention and share valuable insights on what happened in the past twelve months, as well as what to expect for the upcoming year. Topics such as **Fraud-as-a-Service**, **social media fraud**, and **gift card fraud** represent this year's hottest trends, followed closely by more common types of fraud, including **CNP fraud**, **refund abuse**, **first-party misuse**, **bot attacks**, **multi-accounting**, and others.

## This year's highlights

### Key Trends in Ecommerce Fraud

The current economic turmoil, the customers' constant need for a faster and more convenient payment process, as well as the rush of returning to a post-pandemic normal world are some of the many factors that facilitated fraudulent activities in 2022. As ecommerce remains a popular way of shopping for goods and services, fraudsters are bringing new skill sets to the table to make more money off victims' backs. *Fraud-as-a-Service* and *online scams* have become more prevalent in the ecommerce industry, so both merchants and PSPs need to tackle these threats accordingly.

### Fraud Prevention Strategies and Solutions

Being one step ahead of fraudsters means deploying the best fraud prevention strategies and continually improving businesses' solutions, as the fraud environment is constantly evolving. In our second chapter, we analyse some of the most efficient ways to combat fraud while maintaining a smooth customer experience, with the least amount of friction possible.

However, this is hard to be achieved in certain verticals that are often targeted by criminals. The online gambling industry and the travel industry face some of the highest numbers of chargebacks, account takeovers, and red-flagged transactions, which puts extra pressure both on online platforms and anti-fraud solution developers to deliver a state-of-the-art overall customer experience.

Moreover, merchants and fraud solution developers must also keep an eye on the busiest time of the year, the holiday season, as this is too the busiest period for fraudsters – and what better way to deter fraud than by the power of example? Our brief Q&A session will provide valuable insights from key players and anti-fraud specialists who successfully deployed anti-fraud strategies in their businesses.

### Latest Updates on Technology That Helps the Industry Detect and Prevent Fraud

An important part of keeping the payments process safe is deploying the latest technologies to better identify, prevent, or fight fraud before the damage is caused. Our industry experts have laid down the best practices in fraud decisioning, orchestration, and tokenization to effectively deter fraud in ecommerce, without compromising the user's experience.

From mobile commerce fraud to card declines and other common types of fraud, deploying high-end, up-to-date anti-fraud solutions is the only way merchants can maintain a low cart abandonment rate and protect customers when shopping online. Browse this section to find out more about navigating the CX journey across various types of fraud – what merchants can do to ensure high CX satisfaction or how to rescue credit card declines.

### Operations and Costs

Fraud causes the loss of billions for companies – but fighting it properly can also put a strain on their yearly budgets. This section of the report analyses the true costs of deploying efficient anti-fraud systems and technologies, training fraud teams to use a unique combination of data, machine learning, and AI to deter fraudsters, while navigating the shallow waters of an unstable global economic system and downturn. →

# Foreword

## Standards and Compliance

To ensure a high level of security, merchants must go to extreme lengths and provide strong customer authentication without too much friction for the end-user. One way to help merchants maintain low abandonment cart rates and provide maximum user satisfaction is by implementing the latest standards and regulations, including PSD2, PSD3, and SCA. The following chapter focuses on the ever-changing field of anti-fraud regulation and provides the latest updates with valuable input from industry leaders.

## Who Is Who in Fraud Prevention

Our next chapter is dedicated to notable players in the industry who are constantly chasing and deterring fraud by eliminating pain points while adapting to customers' evolving expectations. This year's edition of our report features an overview of key players' core services in fraud prevention.

Finally, solution providers present their approach against the increasing fraud challenges and render us the potential of their latest technologies, their reach in the industry, and their successful business model for the specific target group they serve.

## Our commitment

The main topics tackled in this report are relevant not only in understanding how complex the fraud system is globally but also in determining the most successful strategies end-users, merchants, and PSPs can implement to protect themselves from this phenomenon. We hope the up-to-date perspectives, tips, and insights provided by our specialists will help you better understand and combat fraud in the upcoming year. So, without further ado, we invite you to join us in this journey and explore **The Paypers' Fraud Prevention in Ecommerce Report 2022-2023!**

*Enjoy your reading!*

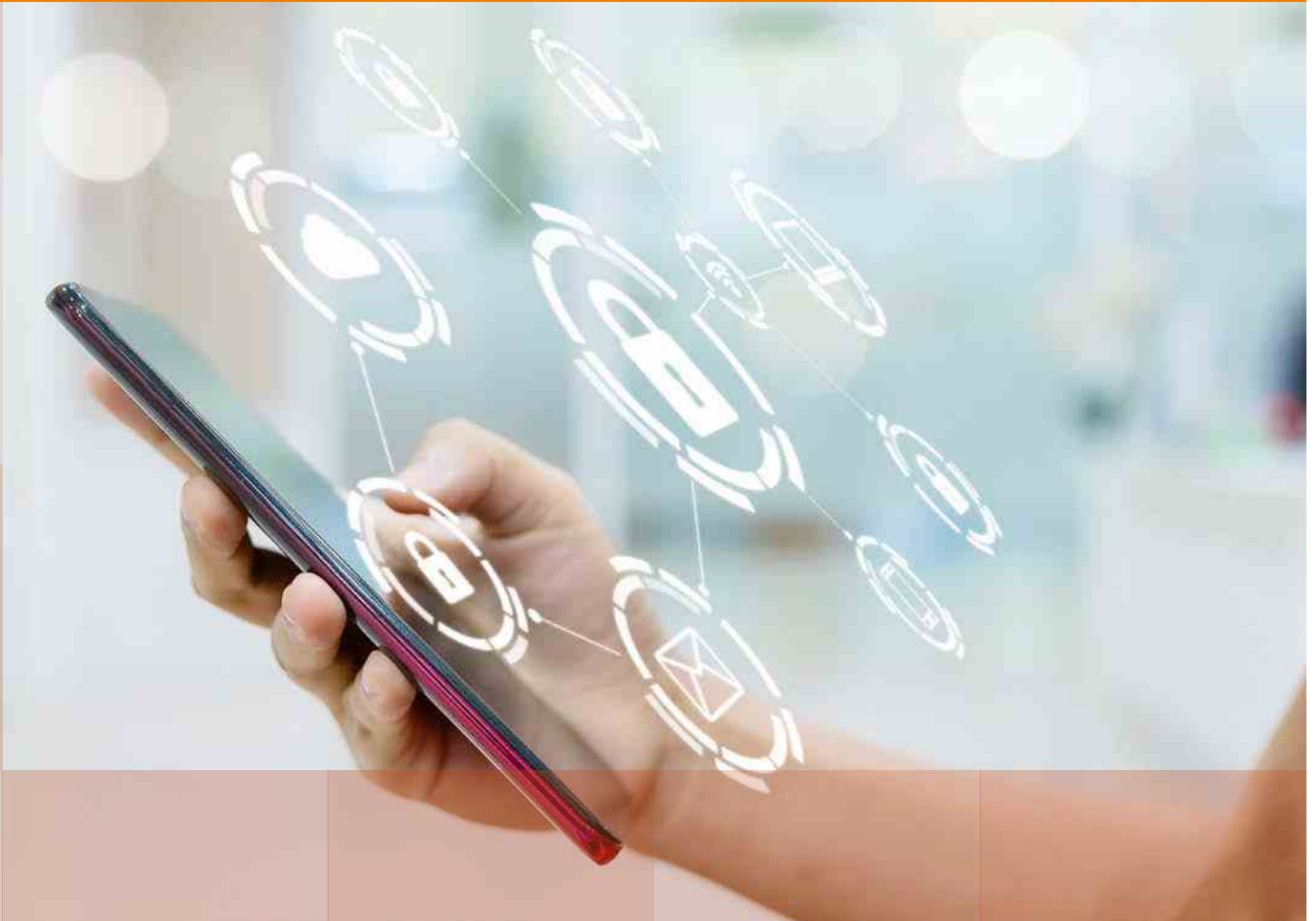
# Table of Contents

3	<b>Foreword</b>
8	<b>Key Trends in Ecommerce Fraud</b>
9	<b>Fraud in Challenging Economical Situations</b>   Interview with Jane Lee, Sift
11	<b>A Year of Change: Updates on the Fight Against First-Party Misuse</b>   Interview with Úna Dillon, MRC
14	<b>Fraud-as-a-Service: How to Wrestle It to the Ground</b>   Steve Hoofring, The Strawhecker Group
16	<b>Online Scams Have Become a Global Epidemic</b>   Jorij Abraham, Global Anti-Scam Alliance
18	<b>Fraud Prevention Strategies and Solutions</b>
19	<b>Fighting Common Types of Fraud by Deploying New Fraud Prevention Solutions</b>
20	<b>How Merchants Can Fight Back in the New Era of Payments Fraud</b>   Augustin Testu, Checkout.com
22	<b>Navigating the CX Journey Across Various Types of Fraud: What Can Merchants Do to Ensure High CX Satisfaction</b>   Alexander Hall, Dispute Defense Consulting
24	<b>Rescuing Credit Card Declines</b>   Channan Lavi, Kipp
26	<b>Mobile Commerce Fraud: A Twisting Hydra</b>   Jumaane Hutchinson, Netcetera
28	<b>The Most Affected Verticals by Fraud</b>
29	<b>Game Over, Fraudsters: How to Fight Fraud in Online Gambling and E-Gaming Industries</b>   Interview with Tony Petrov, Sumsb
31	<b>Best Practices to Fight Ecommerce Fraud</b>   Monica Eaton, Chargebacks911
33	<b>Fraud During the Holiday Season</b>
34	<b>You Better Watch Out! You Better Not Click! – When Cybercriminals Want to Spoil the Holiday Season</b>   Scott Augenbaum
36	<b>Developing a Modern Fraud Strategy in Time for Peak Season</b>   Interview with Domingo Figueira Orihuela, CMSPI
38	<b>Best Practices for Fighting Fraud – Brief Q&amp;A Session</b>
39	<b>The Lay of the Fraud Land – Best Practices</b>   Elena Emelyanova, Wargaming.net
40	<b>The Lay of the Fraud Land – Best Practices</b>   Augie Kennady
41	<b>Latest Updates on Technology That Helps the Industry Detect and Prevent Fraud</b>
42	<b>Fraud Prevention Is Key in the Customer Journey: Differentiating Between Legitimate Users and Bots</b>   Interview with Maciej Pitucha, Nethone
44	<b>Best Practices in Fraud Decisioning and Orchestration That Help Customers Stay Safe</b>   Interview with Maya Ogranovitch Scott, Ping Identity
46	<b>Tokenization and the Fight Against Fraud</b>   Nick Maynard, Juniper Research

# Table of Contents

48	<b>Operations and Costs</b>
49	<b>Proofing Fraud Prevention Management in Times of Economic Downturn</b>   Interview with Amanda Mickleburgh, ACI Worldwide
51	<b>Why Ecommerce Is More Vulnerable to Fraud During Economic Restrains</b>   Darryl Green, CAF
53	<b>Standards and Compliance</b>
54	<b>How to Optimise User Experience While Ensuring a High Level of Security</b>   Claire Deprez-Pipon, Worldline
56	<b>Fighting Fraud Using the Right Tools: How Can PSPs Help Merchants Maximise Conversions</b>   Interview with Okan Ozaltin, Signifyd
58	<b>PSD2 in the UK: the Impact on Fraud and Revenues to Date</b>   Galit Shani-Michel, Forter
60	<b>Who Is Who in Fraud Prevention</b>
61	<b>Overview of Key Players' Core Services in Fraud Prevention</b>
63	<b>Company Profiles</b>

# Key Trends in Ecommerce Fraud



As ecommerce remains the norm of shopping for all goods and services, fraudsters are bringing new skill sets to the table to make more money off victims' backs. In this chapter, we identify some of the latest global fraud trends emerging in ecommerce and how businesses can stay ahead of the fraudsters' game. *Fraud-as-a-Service* and *online scams* have become more prevalent in the ecommerce industry, so both merchants and PSPs need to tackle these threats accordingly.



# Sift

We talked to Jane Lee, Trust and Safety Architect at Sift, about the struggles merchants face amid the current economic context and the holiday season ahead when fighting fraud and adopting the latest fraud prevention solutions.



**Jane Lee** is a Trust and Safety Architect at Sift who specialises in malicious websites, spam, misinformation, account fraud, content abuse, chargebacks, and payments risk. Prior to joining Sift, she was at Facebook and Square, and also spent some time as a private investigator. She is passionate about designing and operationalising systems for detection and enforcement of fraud at scale.

Jane Lee ■ Trust and Safety Architect ■ Sift

## How will the current economic and geopolitical context (high inflation, spikes in prices, environment sustainability, etc.) influence the merchants' activity and fraud levels?

This year, we are expecting merchants to experience a **longer** holiday shopping season. Unfortunately, that will likely come with elevated fraud rates too. Consumers reportedly started making seasonal purchases earlier than usual this year, taking advantage of annual sales and discounts. With inflation rapidly impacting every market, shoppers are aggressively hunting for the best possible prices to deal with rising costs, while still obtaining specific gift items. Because of this increased economic tension among shoppers, they're going to flock to merchants with the most competitive prices.

“The focus for fraud teams this season – and during every holiday shopping period – should be gift card fraud, in addition to account takeover (ATO).”

Despite ongoing supply chain issues and inconsistent inventory, consumers are willing to wait in order to maximise their spend, and will often **reduce non-gift spend** for the sake of having a better holiday experience.

In this disrupted environment, fraudsters rush to take advantage of consumers' need for deals to deploy scams designed to collect fraudulent sales or PII – often both.

## What will be the main types of fraud merchants should expect in this new economical context?

The focus for fraud teams this season – and during every holiday shopping period – should be gift card fraud, in addition to account takeover (ATO). Gift card scams are popular because they're a common purchase during this time and lack proper security features. Additionally, consumers often don't spend the funds right away, giving fraudsters more time to attack.

Account takeover attacks have steadily grown in scale and sophistication over the past few years. Sift found an alarming **131%** rise in ATO attacks in the first half of 2022, a trend set to accelerate over the holidays. Even a single account breach can have long-term impact on a brand – **43% of consumers** said they would stop using a site or app if their associated accounts were compromised by ATO.

Despite spending projections being lower this year, merchants will still deal with higher order volumes than they do during the rest of the year and may have fewer employees to handle the oversight. That's especially problematic if the organisation recently experienced layoffs, had to put a cap on budget, or saw unusually high customer churn as macroeconomic conditions changed. Because holiday shopping typically takes place on known, individual days and during specific shopping hours, fraudsters know they'll have an easier time staying undetected if they target seasonal transactions. →

## What main verticals do you anticipate being the most targeted?

Retail will remain in the crosshairs, especially as companies look to **shed inventory**. **Travel and hospitality** are also expected to have their best year in recent memory thanks to easing pandemic concerns. So, while rising fraud in retail would always be predictable given the time of year, the reason for fraudster's interest in specific verticals, and the way they exploit those verticals, will change based on how the economic and geopolitical landscapes continue to shift.

Less typical holiday targets – like fintech and on-demand services – have recently seen upticks in account takeover fraud, too, and are expected to feel ongoing strain due to market conditions. ATO rates rose by 71% and 39% YoY in those verticals respectively, with a **79% spike in crypto alone**.

## As merchants are already drafting austere budgets for 2023 and considering smaller profit margins, how can they efficiently fight fraud with fewer resources and fewer people?

Firstly, merchants need to maximise what they already have. If existing policies and procedures haven't been scrutinised recently, now is a fantastic time to review them. Strip away the extraneous and focus your fraud efforts on where you know you can get the most ROI.

Automation is also key here. In lieu of human power to fight fraud, leveraging technologies like machine learning is critical to managing holiday volumes, especially considering the longer holiday season we're expecting this year.

## How can Sift's solutions mitigate fraud, chargebacks, volume fluctuations, score, and inconsistent forecasting to ensure a more pleasant shopping experience for customers and help merchants generate more revenue?

Simply put – by learning in real time. If we are operating in a fluid and changing macro-environment, we need technology that adapts in kind. Having the most up-to-date understanding of what is truly fraudulent or legitimate allows us to precisely deploy experiences to the right people. Customers get a more pleasant experience, while fraudsters get the opposite.

Sift also drives significant revenue by securing the accounts customers have with businesses. Most merchants provide customised offers and rewards in their apps, often paired with stored payment credentials to expedite checkout. This is especially important at this time of the year for consumers to get their hands on limited releases and take advantage of flash sales – which are attractive to buyers on a budget. By ensuring access to the accounts that are authorised and trusted, merchants can confidently secure and serve their customers with every engagement.

## And finally, what advice would you give merchants to prepare for 2023?

It feels early, but we should all be preparing for the PSD3 legislative draft coming early next year. While it won't be as monumental a task as adopting PSD2 was in the first place, the **expected clarifications** and updates will affect how we manage payments and customer authentication moving forward. For that reason, optimising your fraud operations with a focused digital trust and safety strategy, and adding automation to your tech stack, will prove extremely helpful as businesses adapt to PSD3.

[Click here for the company profile](#)



[sift.com](https://sift.com)

**Sift** is the leader in Digital Trust & Safety, empowering digital disruptors to Fortune 500 companies to unlock new revenue without risk. Sift dynamically prevents fraud and abuse through industry-leading technology and expertise, an unrivaled global data network of 70 billion events per month, and a commitment to long-term customer partnerships. Global brands such as DoorDash, Kickstarter, Wayfair, and Blockchain.com rely on Sift to gain a competitive advantage in their markets. Visit us at [sift.com](https://sift.com) and follow us on

[LinkedIn](#)

# Merchant Risk Council

The Paypers sat down with Úna Dillon, VP of Global Expansion & Advocacy for the MRC, to walk us through the progress being made on first-party misuse (FPM) and insight into what the future might hold for FPM.



Úna is VP of Global Expansion and Merchant Advocacy at the MRC and was recently appointed to the European Commission Payment Systems Market Expert Group (PSMEG) to advise on regulatory policies on payments and payment fraud prevention.

Úna Dillon ■ VP of Global Expansion and Merchant Advocacy ■ Merchant Risk Council

## Why the change from ‘friendly fraud’ to ‘first-party misuse’?

Simply put, first-party misuse is a more accurate description of what’s actually occurring.

It allows for a more suitable classification and helps merchants reduce their risk of penalties and fines from the card networks in the event they exceed their fraud chargeback thresholds. If a genuine customer knowingly disputes a valid purchase and claims it as fraudulent, it doesn’t make sense for the merchant to be held responsible both for the lost value of the item sold and any penalty as a result of an increased number of fraud-related disputes.

“ Together, we really can make a difference when it comes to first-party misuse; you only have to look at the remarkable progress made over the last year to see the truth in that.

Recontextualising FPM as intentional misuse, as opposed to fraud, helps clarify what’s occurring and that transparency is better for everyone in the long term.

## What are some of the most significant developments in the fight against FPM over the last year?

Probably the biggest and most exciting change is the higher level of active engagement on the part of the card networks.

At the MRC, one of our roles as the Voice of the Merchant is engaging with the card networks on behalf of our merchant members and informing them of the concerns of our mutual customers, the merchants. The issue of FPM wasn’t really on the card networks’ radar until the MRC’s Merchant-Issuer Executive Committee made it one of the top three areas of focus, backed by the issuers and merchants that make up our membership.

Once these problems were raised and elaborated on with data from the **2022 Global Payments and Fraud Report**, major global card issuers like Visa and Mastercard responded relatively quickly. Visa was the first to take a big step in adopting the MRC definition of FPM, and integrated that into a new scheme rule, providing opportunities for merchants to reexamine and represent these disputes. They worked closely with the MRC to develop new processes for merchants to address FPM and for reclassifying the related disputed transactions as misuse instead of inaccurately categorising them as fraud.

Visa’s new rule on the provision of **Compelling Evidence (3.0)** will become effective in April 2023. From then on, merchants will be able to represent these chargebacks and potentially prove the customers in question are misusing the system by reporting fraud when fraud has not occurred. →

Mastercard is following closely behind and is also in discussions with the MRC on the right messaging to include in a similar new rule. It is expected an update will be issued by the network in 2023. Other networks are poised to move in the same direction, so the next year should see a significant change in the FPM landscape due to the networks' positive action.

### The fight against FPM is evolving, but it's not over yet. What are your top recommendations for steps merchants can take today to help address FPM?

One of the most common reasons for customers to dispute transactions in this way is when they don't recognise a transaction narrative on their bank or payment card statement. Instead of contacting the merchant directly to clarify, they contact their card issuer and file a dispute, thereby initiating a costly chargeback with the assumption of fraud.

As a merchant, ensuring your brand name appears as clearly as possible on a customer's statement can go a long way toward correcting the issue. A customer is much more likely to recognise a transaction if they see a merchant's name clearly displayed, and even if they don't, they're more likely to contact the merchant directly with questions.

### What do you think the future of FPM looks like? Can it ever truly be eliminated?

I believe it will become less prevalent as more cardholders learn that engaging in this type of behaviour is wrong and incurs costs that affect the entire ecommerce ecosystem. Claiming a fraud when you know a transaction is genuine is a crime.

Outside of the regular customers doing this, there are Organised Crime Gangs (OCGs) who also avail themselves of the loopholes and weaknesses in the system that facilitate this kind of behaviour. Closing the loophole and making it easier for card issuers to avoid fraud-related chargebacks will help cut down on this OCG activity.

We expect to see those same OCGs exploiting the use of cryptocurrency purchases and Open Banking while there is no dispute resolution process in place yet for consumers using those payments methods.

### Any final thoughts for merchants as they consider a proactive FPM strategy?

Merchants need to talk to each other. Talking to other organisations, not just in your vertical or market, but across ecommerce is profoundly important. It's something we really encourage with our **global communities**, and we work hard to cultivate an environment where payments and fraud prevention professionals can responsibly share ideas and compare notes.

Together, we really can make a difference when it comes to first-party misuse. You only have to look at the remarkable progress made over the last year to see the truth in that.



[merchantriskcouncil.org](https://merchantriskcouncil.org)

The **MRC** is a global non-profit membership association connecting ecommerce payments and fraud prevention professionals through educational programs, online community groups, conferences, and networking events.



## MRC's Essential Online Courses for Payments and Fraud Prevention Professionals



# 1 YEAR ALL ACCESS PASS BEST VALUE

Get unlimited access to the entire entire catalog of high-quality, accredited eLearning courses - including any new courses that launch while your pass is active.

Perfect for training your team or revisiting the fundamentals at an unbeatable price!

SCAN HERE



## LEARN MORE TODAY

Expand your knowledge at your own pace. Enroll in our online courses:



**CHARGEBACK ESSENTIALS**



**FRAUD ESSENTIALS**



**PAYMENT ESSENTIALS**



**EMV 3DS AUTHENTICATION ESSENTIALS**



**BUY NOW, PAY LATER ESSENTIALS**



**FIRST-PARTY MISUSE ESSENTIALS**



**MACHINE LEARNING FOR FRAUD PREVENTION**



**CRYPTOCURRENCY ESSENTIALS**

...with more courses coming soon!

## Fraud-as-a-Service: How to Wrestle It to the Ground



**Steve Hoofring**, Senior Associate, is a technology and operational executive in the payments industry with over 20 years of experience. Steve helps deliver services that include strategic planning, buy-sell side services, market intelligence and research, industry and business specific analytical research, product benchmarking and performance, product development and business implementation services.

**Steve Hoofring** ■ *Senior Associate* ■ TSG (The Strawhecker Group))

For context, let's assume John is ordering a high-performance exhaust, delivered to his neighbor, using a stolen card. He can sell it for USD 800 and has the order. His neighbour wants USD 100 for the address, which is a good win for him and his customers. Suzy also has a great business selling stolen children's clothes from a top-five retailer. Using stolen checking accounts, she orders online and sells both locally and online, once she receives the goods.

Winning the battle of fraud is critical for your business. To do so it's important to know your fraudsters. How many are there? Where do they live? Understanding their habits will help you win the battle. And, with Fraud-as-a-Service (FaaS) continuing to increase, especially in card not present transactions, it's critical for your team to get close.

Today's fraudsters have become more professional and sophisticated. Using FaaS resources on the Dark Web and fraud-related blogs gives them access to more customer data, even comprehensive data like a social media profile, and they can impersonate more customers, more quickly to steal. And they will, as it is their job. Each day they get up and go to work, some in teams, just like you. So, study your losses closely. Learn their patterns and introduce that data into your fraud systems.

### Work the data

There are always trends and recurrences. To help find and stop the fraudster it is important to view the battlefield, not just the incident.

Extract data, span timelines, isolate by location or geography. Getting down to the details is important to avoid punishing good customers and catching the bad ones. Avoid being constrained by just the tools you have. Get the data, then use it to engage other resources to stop the behaviour and build new tools. If you can change the economics for the fraudsters, they will be less likely to stay and will, eventually, move on.

A fraudulent transaction will cost your company up to 2.5 times more than the actual cost of goods and services. So, stopping fraud provides value to your organisation that is not always immediately recognised. When you stop fraud in your organisation, celebrate the victory. Globally, half the online businesses have experienced some fraud, so we are all in this together. Consider joining an organisation like the Merchant Risk Council (MRC), where working together and sharing benefits all. Moreover, sharing your learnings helps other businesses win as well. It may be tough work, but it could also prove rewarding, especially since you will help building a stronger anti-fraud system that, ultimately, will benefit both end-customers and merchants.

### Squeeze the middle

Eric's Risk tool allows him to look at risky orders before they ship. His company ships his product quickly, but his fraud tools set some transactions to 'maybe'. It's a 'yes' to the customer but 'maybe' orders are on hold until he releases them. →

If your tools put transactions into three categories – yes, maybe, and no – you should work hard and focus on the 'maybes.' Not just confirming and releasing orders but determining why it was a 'maybe' and how can you judge between was it right or wrong. More importantly is finding why is it wrong. False positives can lead to serious impacts to your customers.

Once, we declined a Prime Minister's spouse at the airport. That call was not easy, but the experience taught us to really focus on the False Positives and 'Squeezing the Middle'. What your company can do is dig into that data and see if you can use it to improve your tools. That's what 'squeezing the middle' means – working around the transactions flagged as 'maybe' and determining whether they are legitimate or not. By doing so, merchants not only enhance their customer's satisfaction rate but can also drive sale and become a most trustworthy merchant for customers.

### It's a journey

Today, there are great companies providing equally great services to detect and stop fraud. These companies have both the knowledge and data to help merchants fight it.

TSG has worked in both real-time and batch fraud tools to help businesses fight fraud. If businesses have a problem and lack the resources to stop theft, they should find the right vendors that can help. When finding the right fraud prevention tool, it is important to take action as soon as possible, since fraudsters count on merchants' slow response rate and, once they find that gap, they will move as quickly as they can. Merchants should be nimble, efficient, and know their fraudsters.



[tsgpayments.com](https://tsgpayments.com)

**TSG (The Strawhecker Group)** is a globally recognised analytics and consulting firm that supports the entire payments ecosystem, serving over 1,000 clients from Fortune 500 leaders to more than a dozen of the world's most valuable brands. Trusted by industry leaders, TSG's strategic services, market intelligence, and analytics merge to empower clients with actionable and accessible information.

# GASA (Global Anti Scam Alliance)

## Online Scams Have Become a Global Epidemic



**Jorij Abraham** has been part of the international ecommerce community since 1997. He has been an ecommerce manager at Bijenkorf, TUI, an online publisher at Sanoma Media, and Director of Consulting at Unic. He also co-founded two companies: eVentures Europe and vZine. From 2013-2017 Jorij has been Director of Research & Advise at Thuiswinkel.org and Ecommerce Europe. Since 2017 he runs the Global Anti Scam Alliance and [ScamAdviser.com](https://www.scamadviser.com).

**Jorij Abraham** ■ *General Manager* ■ [ScamAdviser.com](https://www.scamadviser.com) and The Global Anti-Scam Alliance

Scammers have proven more successful in 2021 than ever before. The number of scams reported increased by 10.2% from 266, in 2020, to 293 million reports in 2021. Scammers use any crisis to scam people. Moving from pre-ordering COVID-19 vaccination at the beginning of 2021, to cheap flight tickets for Hajj pilgrims, 'supporting' victims from the Australian bushfires, 'helping' Ukrainian refugees, and, more recently, tickets to Queen Elizabeth's funeral memorial and government energy grants.

### The bloody facts

With 4.72 billion internet users, **60.1% of the global population** is now spending nearly seven hours every day online, pushing the economy towards digitalisation at an increasing rate. Under this climate, crime is following quickly, with most Western countries reporting that online scams are now the most reported type of crime.

According to the Australian Competition and Consumer Authority (ACCC), 96% of Australians have been exposed to a scam in the last 5 years with half of these contacted weekly or daily by scammers. In the UK, 50% of TCSEW respondents reported receiving an email, text, or social media message that may have been phishing.

### Figure 1: Scams are in many countries now the most reported type of crime

### No longer a Western disease

Scams are no longer a Western disease. 53% of Filipinos stated they were targeted by fraudsters in three months' time, with 11% of them ending up as victims. Similarly, other developing countries including Brazil, Ghana, Nigeria, and Kenya reported increases in online scams, especially via mobile phones.

In Nigeria, the number of transactions via mobile channels increased by 164% in 2021, and, as a result, mobile scams boomed as well. 62% of Saudi Arabia consumers received spam and scam messages, mainly on their mobiles and 14% admitted falling for the scam and losing money. In South Africa, two massive data breaches caused a tsunami of phishing attacks using highly personal data. Indonesia reports that 25% of its citizens have been a victim of online fraud, making it the second-largest reported type of crime in the country. →



## Social media – the stepping stone for scammers

In nearly all countries, social media platforms are plagued by scammers trying to lure victims. According to Pakistani authorities, 23% of the online crime complaints received start on Facebook. Indonesia states that 51% of the scams start on social media, while in the US, more than one in four people who reported losing money to fraud in 2021 claimed it started on social media with an ad, a post, or a message.

There seems to be a trend to make social media more accountable. ACCC is taking legal action over alleged misleading conduct by Meta for publishing scam celebrity crypto ads on Facebook. On a positive note, in Malaysia, Meta is supporting an online scam awareness campaign.

## Get them while they're young

Another scam trend several countries, like Brazil, China, Finland, the Netherlands, New Zealand, and Thailand are reporting, is that young people are targeted more and lose more frequent money than the elderly. However, seniors still lose the most money, especially to investment/ crypto scams.

In Finland, students seem to be a targeted group. The worst-hit age group was individuals between 18 and 30 years old (23.3%), who were scammed 8% more, compared to 2020. New Zealand reports that 55% of the people who call out scams are 40, while a study from Thailand shows that Generation Y and Z are the most vulnerable to online scams due to the amount of time they spend online.

Similarly, a Chinese survey of college students reported that more than a tenth of the respondents lost money to scammers, which prompted the Chinese government to launch a new wave of education campaigns aimed at making young adults more wary.

## Scamming as an industry

Scams have been industrialising for years. In a recent development, Taiwanese and Chinese citizens are tricked by human traffickers who are mainly targeting young Asian people via social media, offering

well-paid work and accommodation in countries like Cambodia, Thailand, Myanmar, and Laos. On arrival, their passports are taken, and they are sold to different groups and forced to work in offices running illegal phone or online scams. Taiwan authorities claim almost 5,000 citizens were recorded travelling to Cambodia and not returning.

Another development is the rapid growth of SaaS (**Scam-as-a-Service**). Scams are automated and increasingly fine-tuned to specific target groups. Scam scripts (websites) are developed and distributed to local scam organisations. Cybercriminals also professionalise in specific specialisations (traffic generation via social media, text, and email spamming, cryptocurrency laundering, retargeting of scam victims).

Similar to private companies such as **ScamAdviser.com** and **Trend Micro**, more countries are starting to offer tools to their citizens to check for malicious websites, email addresses, bank accounts, cryptocurrency addresses, and phone numbers. Malaysia is taking this one step further by offering a search engine and app that allows the public to check phone and bank account numbers used by crime syndicates.

## The cure for scams?

Available data shows that only **0.05% of all cybercrimes are prosecuted**. Raising awareness is not enough. Prevention could take the form of a global sharing system of scam data (be it domains, email addresses, cryptocurrency addresses, or bank accounts). The data would only be used by consumers to assess the risk of being scammed, but also to proactively block or take down malicious assets.

National initiatives like those of the Belgium Cybersecurity Center, where consumers can forward phishing emails and data is used in real-time to block websites have already proven to reduce the number of scams. The next step is taking these kinds of initiatives internationally.



[gasa.org](https://gasa.org)

The mission of the **Global Anti Scam Alliance (GASA)** is to protect consumers worldwide from scams by raising awareness, enabling hands-on tools for consumers and law enforcement, facilitating knowledge sharing, organising research, supporting the development of (legal) best practices, and offering training and education. To find answers, GASA is organising the **Global Anti Scam Summit** to define concrete actions to combat online fraud.

# Fraud Prevention Strategies and Solutions



## FRAUD PREVENTION

Being one step ahead of fraudsters means deploying the best fraud prevention strategies and continually improving businesses' solutions, as the fraud environment is constantly evolving. In this chapter, we analyse some of the most efficient ways to combat fraud in high-risk verticals such as online gambling or travel, while maintaining a smooth customer experience, with the least amount of friction possible.

We also put together a brief Q&A session in order to provide valuable insights from key players and anti-fraud specialists who successfully deployed their latest anti-fraud strategies in their businesses.

# Fighting Common Types of Fraud by Deploying New Fraud Prevention Solutions



From mobile commerce fraud to card declines and other common types of fraud, deploying high-end, up-to-date anti-fraud solutions is the only way merchants can maintain a low cart abandonment rate and protect customers when shopping online.

# Checkout.com

## How Merchants Can Fight Back in the New Era of Payments Fraud



**Augustin Testu** is a Senior Product Manager at Checkout.com, responsible for building products that empower merchants to fight fraudulent threats without compromising payments performance. Prior to joining Checkout.com, Augustin held product management roles at Ant Group and World First.

Augustin Testu ■ Senior Product Manager ■ Checkout.com

Online payment fraud is rising fast. In 2021 alone, it increased by **285%** as fraudsters exploited the growing volume of online commerce and weaknesses in businesses' fraud defenses. And the threats continue to evolve, with devastating impact: it's estimated online sellers will experience losses exceeding USD **206 billion** between 2021 and 2025.

Fraudsters are also becoming more sophisticated. Automated attacks, primarily through bots, are major new threats businesses face. These attacks make it easy for fraudsters to scale their efforts. For example, it can **cost less than USD 200** to attempt 100,000 account takeovers, with a success rate between 0.2 and 2%.

Also, the threat is not uniform. Fraudsters go after different businesses in different ways. Ecommerce, airline ticketing, money transfer, and banking services businesses seem **more vulnerable** to credential stuffing and account takeovers. Online marketplaces are **primarily targeted** by fake accounts, false advertising, order cancellations, and fake buyer/seller closed-loops.

The crypto sector gets hit with fake exchanges, wallet takeovers, and **Man-in-the-Middle Attacks** (MITM). Online gaming businesses suffer most from fake third-party top-up services, credential stuffing, account takeovers, and Streaming Potluck schemes.

*19% of retailers say they have suffered significant amounts of other payment fraud in the past six months.*

A rigid, one-size-fits-all approach to fraud is no longer enough in this new fraud paradigm. Businesses must deploy sophisticated fraud management strategies that take a more nuanced approach to balance risk and maximise revenue. And to do that, they need solutions that:

**Leverage millions of data points:** Merchants need the power of advanced machine learning that detects new fraudulent trends and uses network-wide intelligence in real time. The more data points the fraud solution can call upon, the better it can learn from patterns of real fraud across multiple sectors and countries and apply these insights to identify and stop suspicious activity at the point of transaction. Without these comprehensive insights, merchants are left exposed to emerging fraud patterns.

**Provide complete customisation:** Merchants not only want to define their overall risk tolerance but also tailor fraud strategies for specific segments or criteria. For example, a merchant will probably deem a returning customer using the same IP address, buying something expensive as 'safer' than a new customer from a flagged IP address buying something of lower value.

Merchants need the flexibility to treat these two transactions with different risk classifications and to build tailored fraud strategies for each. They also need to do that across multiple segments – to separate high-risk versus low-risk geographies, segment by different payment methods, or even detach specific product codes that experience more fraud attacks than others. Merchants must be armed with unlimited scope to create rules that suit the specifics of their business. →

As well as setting individual fraud thresholds for different segments, merchants should have more control over the action triggered when a threshold isn't met (e.g., accept or decline, send to 3DS, or undertake a manual review). These actions provide merchants with additional levers to block more fraud or reduce strictness to allow more transactions through.

**Allow for continuous optimisation:** To stay one step ahead of the fraudsters, merchants need access to powerful analytics and testing capabilities to fine-tune strategies and inform new ones. Desired capabilities include highly visual illustrations of current risk strategies that merchants can adjust by adding, amending, or subtracting components.

Merchants should also demand a centralised view of all transactions requiring manual review, alongside rich contextual data on why each transaction has been flagged, saving time, and increasing the accuracy of decisions. And for each change, merchants must be able to experiment safely with new rules by testing their potential before pushing live.

### Fight fraud without harming the customer experience

Fighting fraud shouldn't be an overly defensive exercise. Instead, it should maximise revenue by increasing acceptance rates and reducing friction for legitimate customers, leading to more conversions. **Research** from Checkout.com found a declined payment has permanently put that 34% of people off an ecommerce store, but a much higher 52% will abandon their baskets if the payment process is too complex.

Many fraud tools today mandate strict risk strategies that create friction and frustrate customers. Merchants need solutions that work with the customer experience. They must be able to monitor the impact of their risk strategies on key metrics, such as conversion, acceptance rates, and performance against scheme chargeback limits. They must be able to do that within the safety of a testing environment while also investigating and diagnosing the root causes of false positives and false negatives and using these insights to eliminate burdensome anti-fraud measures.

### Futureproof the fight

Fraud is ever developing, as are customers' expectations about what makes a great shopping experience. Merchants that stay ahead will be those that recognise this is not a zero-sum game and that you can fight fraud *and* prioritise sales. The right solution must protect them today and from whatever future fraud throws their way.

Checkout.com's new Fraud Detection Pro empowers complex global businesses with an advanced suite of tools to fight fraudulent threats without compromising payments performance. To learn more, visit [checkout.com/products/fraud-detection](https://checkout.com/products/fraud-detection).



**Checkout.com** is a global payments solution provider that helps businesses and their communities thrive in the digital economy. It offers innovative solutions that flex to your needs, valuable insights that help you get smart about your payments' performance, and expertise you can count on as you navigate the complexities of an ever-shifting world.

[checkout.com](https://checkout.com)

# Dispute Defense Consulting

## Navigating the CX Journey Across Various Types of Fraud: What Can Merchants Do to Ensure High CX Satisfaction



**Alexander Hall** is the owner of Dispute Defense Consulting and the host of the Fraud Prevention Roundtable Series. He has 15 years of fraud-related experience, 10 of which were spent operating as a fraudster. During that time, his methods were deployed against businesses across all industries and caused 10's of millions in damages. In 2017, following the birth of his daughter, Alexander joined the ranks of fraud prevention. In 2020, Alexander founded Dispute Defense Consulting. DDC works with merchants, banks, vendors and publications in varying capacities to secure transactions across the global marketplace.

Alexander Hall ■ Founder ■ Dispute Defense Consulting

For those who are looking to catalogue the number of identified fraud methods, it can quickly grow to staggering heights. Investopedia created a list of **eight categories**, each with its own subset of iterations and flavours.

The most common practices (such as dark web carding) are relatively simple to get going. A crypto wallet, a computer with an Internet connection, and guidance provided by a damaged moral compass will get an entry-level fraudster up and running and causing damage totalling more than USD 5.8 billion, a 70% increase between 2020 and 2021, **according to the FTC**.

Conversely, methods that require long-winded manipulation of data (i.e., identity theft and the establishment of new credit cards) take time and deep knowledge of how the systems work and the requirements that each stage requires. **AARP (in collaboration with Javelin) reported that victims of identity theft lost USD 52 billion**.

Data breaches have also become a regular occurrence, affecting virtually every platform that stores information. The information leaked by these breaches supports criminal operations while also flooding the black market and leading to account takeovers (ATOs), identity theft, payment fraud, etc.

Looking at the entirety of fraud, we can identify a throughline that applies to most of the methods: interaction with various touchpoints across a Customer Experience (CX) Journey.

### What are the touchpoints in a CX Journey?

The touchpoints of an operation would include any interaction wherein the user has an opportunity to create a request that would affect a part of the platform. Common examples include account creation, transactions, fulfilment adjustments, transfers, account changes, chargebacks, and refunds/ returns.

**1. Session start:** The moment a user enters an online platform, be it a website, an app, a kiosk, or a video game. At this point, the data points that can be applied towards a later determination are heavily centred around session data such as device fingerprinting and behavioural analytics.

*Methods that can be identified at this point include bot attacks and high-velocity attacks.*

Available Datasets: Device Fingerprinting, Behavioural Analytics.

**2. Account creation** or the first point across the CX Journey that a user identifies themselves. Depending on the provider's industry, the set of the requested information might include name, phone number, SSN/ EIN, email address, and billing/ shipping address. Fraud teams can leverage the device information and behavioural information from the first touchpoint along with submitted PII to start making determinations. →

Methods that can be identified at this point include identity theft, stolen payment information, account takeover attempts, duplicate profile attempts, and more.

Available Datasets: Device Fingerprinting, Behavioural Analytics, Personal Identifiable Information (PII), payment information, biometrics (voice/ face/ fingerprint).

**3. Checkout/ deposits:** Payment information is used to transact with the platform. It is expected to see payment information and the need to evaluate whether the transaction should be honoured, escalated, or declined. The checkout form is an opportunity to collect and verify credit card details, bank account details (for ACH payments/ deposits), gift card details, and more.

Methods that can be identified at this point include carding/ card testing, wire fraud, ATO attempts, discount/ promotion abuse, and gift card fraud.

**4. Customer service/sales/help desk.** Customer-facing agents communicate directly with users via service tickets, emails, phone calls, in-person meetings, social media messages, and more. Each agent has a set of abilities and, therefore, can be targeted by savvy fraudsters. Depending on the authority and access of the agent, most of the methods listed above might come into play.

Methods that can be identified at this point include: carding/card testing, account takeovers, discount/promotion abuse, gift card fraud, automated website security bypasses, account creation, identity theft, scams leading to data breaches (phishing), and others.

**5. Chargebacks:** They monitor the performance of true fraud and operational failures. The fraudulent method is unique because the fraud is deployed by the account holder. This system is exploited by account holders who wrongfully file chargebacks against a company. There are several reasons that might lead to this behaviour, but the

over-arching story revolves around good customers doing bad things, negatively affecting merchants by abusing the chargeback system.

Common terms describing this method are friendly fraud, first-party fraud, or chargeback abuse.

The five touchpoints outlined above provide a high-level perspective on the most common types of fraud found across various industries and serve to illustrate the need for what has been called a 'holistic fraud prevention strategy'. When working with merchants, these following items provide a strong foundation for a fraud prevention strategy that covers all touchpoints across a CX Journey.

### 1. The Identification of all touchpoints wherein a user might influence the operation of a company.

There are countless methods that can be applied against a company, but most of them require either submitted information or back-end device monitoring that can support accurate determinations downstream. By thoroughly identifying the touchpoints that a user has access to, an operator can quickly and accurately identify fraud methods.

### 2. The use of an expansive data set.

Most common include biometrics (voice, facial, fingerprint), device fingerprinting, behavioural analytics, PII, and more. At each stage, different data becomes available either by monitoring the user throughout the session or by reviewing and verifying the information that the user submits. Depending on the industry of the company, regulations and compliance might limit the choices regarding which data sets can be deployed in your system.

### 3. Automation and escalation.

For high-volume companies, working with vendors that provide expansive data sources can afford your team the ability to achieve higher accuracy, while removing unnecessary friction for your good customers.



[disputedefenseconsulting.com](https://disputedefenseconsulting.com)

**Dispute Defense Consulting** provides fraud prevention training and strategy development consulting to companies transacting in the card not present space. With a growing portfolio including recognisable brands from across the marketplace, Dispute Defense has successfully mitigated losses stemming from account takeovers, identity theft, transaction fraud, chargeback abuse and more.

# Kipp

## Rescuing Credit Card Declines



**Chanan** is an experienced payment expert. Before founding Kipp, he held senior positions that included e-payments management, optimisation, and Business Development roles for leading merchant and financial companies. Chanan holds an MA in Economics and MBA from the Jerusalem Hebrew University.

Chanan Lavi ■ CEO & Co-Founder ■ Kipp

Unnecessary declines of credit card transactions for online purchases frustrates three parties:

- The customer, who spent time researching a product for features and price, filling a shopping cart, and checking out — only to be told (without explanation) that they can't complete the purchase.
- The merchant, who invested in building a sales funnel, marketing campaigns, branding, maintaining the site, and expensive customer service, only to lose that sale at the very final stage.
- The issuer, who lost the commission purchase from someone who has chosen that specific card over another and may very well demote that card in their wallet, both at this store and at others.

The source of these declines? The fraud prevention systems used by card issuers to protect themselves from fraudulent transactions and chargebacks. While some are obviously valid, many rejections aren't justified.

### A necessary evil?

The phenomenon of sacrificing a given fraction of transactions is not a necessary, dismissible 'cost of doing business'; it represents a substantial financial loss. How ubiquitous is it?

1. In a recent **survey conducted by Profitwell**, credit card declines were the single largest reason for customer churn among B2B subscription businesses, accounting for 20-40% of the churn and cancellations.
2. Merchants experienced more fraud in 2021 than in 2020, with new types of fraud affecting **62% of merchants**. And, with that increase, so does the number of declines.
3. Even worse, they don't get a second chance; the average merchant only recovers **one in three** declined credit card transactions.

4. It's estimated that false declines will grow to **a staggering USD 443 billion** by the end of 2022. That's not the cost of all declines (some justified) but only the sum that could, and should, have been saved by issuers leveraging a more effective fraud prevention strategy.

There's a good reason why this happens – issuers expect their fraud prevention software to protect them, erring on the side of minimising risk when there isn't sufficient data.

### Sample scenario for each stage

Each of the following sentences represents a helpful data point in assessing fraud – but only *some* are available to the issuer.

A frequent business traveller loses her laptop. She received it as a gift (the issuer doesn't consider her, let's call her Anna, as a big spender), and, before this trip, she visited an office supply website to purchase accessories herself, as well as some small travel items for her 'on-the-go' office. Anna now needs a new machine. Using her phone, she visits that same online office supply store – to order a new laptop to be delivered overnight to her hotel room, in Berlin.

Her transaction is rejected, and she no idea why. She has the money. She hasn't done anything wrong. She's got meetings to attend and no time to troubleshoot this. →



From the issuer's perspective, there is a large purchase, uncharacteristic of the customer's typical pattern. It seems that she just used her card in a German clothing store, far from her home city, and laptops are a category that criminals prefer, as they are relatively small and easy to resell. This customer has instantly joined a massive number of people who will experience the same frustration: in March 2022, **30% of those experiencing declines did so from 'Activity thought to be suspicious'**.

The result? The customer visits the nearest mall, purchasing the laptop with another credit card, just to make sure it'll go through this time. She has now wasted time, paid more for the product, and both the merchant and the issuer lost revenue. The competition — the mall store owner and another issuer — makes the sale with no effort or investment whatsoever.

We understand the issuer's analysis and rejection. But there's a strategy that can sharpen this picture, moving the transaction from the hazy 'grey area' into a safer category. *It's all about data that comes from the merchant.*

### The data is there. It's time to use it to save the sale

Her office supply e-store, for example, knows that:

- The customer has been shopping with them for years;
- Shows no declined charges or abandoned carts;
- She has recently bought that extra mouse and laptop bag, indicating she's using it;
- She has purchased overseas a number of times with a different card;
- She has always worked with the same device ID which matches the device ID she uses on the issuer's app.

These clues provide enough confidence, assuming the merchant can share them with the issuer, to drop the risk level significantly. If merchants had an easy way to interact with issuers, this is one of the many ways they could work together for mutual interests.

### There is no black and white. Let's shrink the grey

Merchants can increase issuer authorisation rates with **Kipp's platform**, where they can collaborate and share data with issuers to reduce both fraud and insufficient fund declines. The enriched data, together with the ability of the merchant to participate in the cost of the issuer risk, reduce the rate of unnecessary declines and allows the issuer to approve more transactions. Only by having merchants and issuer banks working together can their data create a more effective decision-making process.

[Click here for the company profile](#)

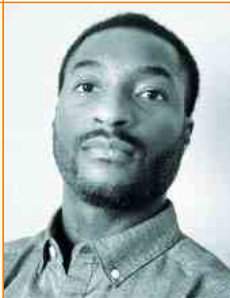


[letskip.com](https://letskip.com)

**Kipp** is a global fintech company enabling issuing banks and merchants to jointly approve legitimate transactions that are currently being declined. The company's platform optimises the traditional payment model for increased revenue, customer satisfaction, and loyalty. Kipp's founders and team are fintech veterans and payment optimisation professionals.

# Netcetera

## Mobile Commerce Fraud: A Twisting Hydra



**Jumaane Hutchinson** is Head of Product for Mobile Wallet and Banking at Netcetera, supporting companies to improve and innovate their digital mobile propositions. Jumaane has vast experience in managing and developing mobile-focused products within the financial services industry. A Computer Science graduate, he developed a keen interest in developing technical products and a passion for product management.

**Jumaane Hutchinson** ■ *Head of Product for Mobile Wallet and Banking* ■ Netcetera

With the rise of mobile devices used for every aspect of our lives, the possibility of mobile fraud has also increased. Especially in the ecommerce field, many new options are now available for fraudsters to target mobile users, and PSPs need to constantly be on the lookout to protect users and themselves against attacks. Here is how some of the new fraud attacks could look like and what we can do to prevent them.

### What is mobile fraud?

The ecommerce space is rife with fraudsters looking to skim customer data and use it for online purchases. In this area, we have seen many different forms of fraud, including identity theft, chargeback fraud, and friendly fraud.



Being able to shop from your smartphone or other devices is a relatively new development and, so, mobile fraud comes from fraudsters trying to take advantage of gaps in mobile security. Between 2011 and 2020, payment fraud **tripled globally**.

Particularly during the COVID-19 pandemic, mobile and online purchases surged for hygienic reasons, and have not abated. Mobile payments are projected to reach USD 2.1 trillion in **2023** and, with that, comes a wider window for mobile payment fraud. Let's take a look at a few examples of how this was presented:

### Account takeover

Account takeover or ATO is the most well-known type of fraud in the online space and remains the most prevalent. The particular danger lies in cases where financial or government account credentials are stolen. This can be done in several ways, e.g., phishing, credential stuffing, man-in-the-middle attacks, etc.

### Merchant identity fraud

There are several ways fraudsters try to impersonate merchants. In the mobile context, it can take the form of rogue mobile apps that mimic genuine ones or false online shops.

### Short links

Short links are used more and more in mobile contexts where there may not be space to display a long URL. Especially with the advent of QR code payments, it has become harder for consumers to verify whether they are following a valid link or a false one that makes it easier for their data to be pirated. The end result of these techniques is always the same – fraudsters gain access to the funds and personal data of end users. →

## How can we prevent it?

There are several measures that online businesses and merchants can take to protect themselves and their customers from targeted mobile fraud.

Firstly, having a robust payment security system is a good starting point. Besides from complying with mandatory PCI and PSD2 requirements, including components that ensure two-factor authentication is paramount. These can include 3-D Secure or newer options like **Delegated Authentication**. Related to this is network tokenization, which is a type of technology that replaces PANs with a representative token, reducing the use of PANs during the payment process.

**Click to Pay** is another option with which PANs can be cloaked altogether. On the authentication side, merchants can also offer biometric options to clients, as an alternative to passwords. Using options such as facial recognition, hand geometry, and voice recognition may be easier and faster for mobile users and harder for fraudsters to fake.

Using a dedicated fraud engine such as risk-based authentication (RBA) is another tool in a merchant's arsenal. This AI engine automatically assesses each log-in or transaction based on the prior behaviour of the customer, i.e., customer behavioural analytics. Other fraud prevention engines include link analysis and graph databases, providing information on flagged cards and devices, and adding an extra layer of security.

Finally, merchants can also encourage customers to follow simple anti-fraud measures, such as checking that they are shopping using a legitimate URL with an SSL certificate, using a security scanner on their device, and not downloading apps that are not from an official Apple or Android app store.

## Lessons learned

The increased rates of fraud and cybercrime in the last few years have only shown that we cannot rest on our laurels when it comes to fraud protection and prevention. Fraud methods have changed and are ever-evolving, which means we need to take a multifaceted and collaborative approach to prevent it. It is also very important to analyse the customer journey to identify possible gaps in fraud prevention measures. For this reason, it is best to not stick to only one form of fraud prevention, but a combination of different tools.

With the holidays coming up and big retail events such as Black Friday, there will be a surge of potential sales and transactions in the months to come. To ensure that you maximise your business and avoid cyberattacks, you should optimise your mobile offering and make sure your defences are sharpened against mobile fraud.

Not sure where to start, or feel like your fraud defence could be better? Don't hesitate to reach out to the **Netcetera team**. We're happy to advise you on any of the aspects above.

[Click here for the company profile](#)

**netcetera**

[netcetera.com](https://netcetera.com)

**Netcetera** is a global software company providing individual digital solutions in the areas of secure digital payment, financial technologies, media, transport, healthcare, and insurance. More than 2,000 banks and issuers, and 150,000 merchants rely on their digital payment solutions.

# The Most Affected Verticals by Fraud



Fraud affects all sectors of the global economy, but some verticals are more prone to face significant losses because of it. Our experts share the threats facing the gambling industry and travelling and provide thoughtful insights on how merchants can stay ahead of fraudsters, chargebacks, and multi-accounting.

# Sumsub

We sat down with Tony Petrov, Chief Legal Officer at Sumsub, and reviewed the most common types of fraud emerging in the online gambling and e-gaming industries, as well as the efficient ways to deter fraudsters while remaining compliant.



**Tony Petrov** was appointed as Chief Legal Officer at Sumsub in 2018. He is an experienced blockchain and fintech attorney with a focus on AML and KYC compliance, data privacy, and international regulator relations. Tony holds a master's degree in Transnational Business Law from the University of the Pacific, McGeorge School of Law in Sacramento, California. A certified CySEC AML Compliance Officer, he is the author and host of the **Sumsub for experts' YouTube channel**.

Tony Petrov ■ Chief Legal Officer ■ Sumsub

## How does fraud affect online gambling and the e-gaming industries?

The gaming industry is experiencing explosive growth and is forecast to reach **EUR 140.05 billion** between 2021 and 2026, with a compound annual growth rate (CAGR) of approximately 11% over the forecast period. And, with rapid growth comes greater exposure to different types of fraud attacks.

“ Even one undetected case of fraud leads to fines unless you have robust verification policies and can prove that this specific case was just an exception within the margin of error.

Since gambling platforms aim to onboard more users as fast as possible, they can also neglect compliance and security requirements, allowing fraudsters easy access to their platforms. The most common AML failures and fraud attacks relate to ineffective threshold triggers and inappropriate controls, multi-accounting, credit card, and chargeback fraud. These failures caused a trend of increasing fines in recent years. For instance, the total amount of fines issued in 2021 exceeded GBP 40 million, and this year's total has already passed **GBP 44 million**, with an enormous fine (or rather a settlement) of **GBP 17 million issued by UKGC** to British gambling platform Entain. We're also seeing bigger fines due to social responsibility failures, such as companies being unresponsive to customers exhibiting

indicators of harm. So, we can expect to see a continuing regulatory focus on the sector's compliance agenda and more scrutiny when it comes to monitoring the operations of industry players.

## What are the most common types of fraud merchants experience in these verticals?

The prevalence of fraud in gambling depends on its type. The most common is multi-accounting (when one person owns two and more accounts, registered for fake/stolen IDs), which is used for *gnoming* (betting on the most probable outcomes of one game through different accounts), chip dumping (joining games from multiple accounts and deliberately losing money to one of those accounts), and bonus abuse (exploiting the bonus policy of the gambling company), which can lead to more than 50% revenue loss (Marketline, 2021).

Credit card fraud and chargeback fraud are also quite common in the gambling industry. Nearly **90%** of all chargebacks are considered friendly fraud, which results in direct revenue loss and payment processor fees, as well as reputational consequences.

Money laundering is another problem in the industry, with perpetrators using the same methods mentioned above. 'Dirty' money is deposited on the gambling platform, the fraudster plays a couple of games and then withdraws the money, claiming it to be gambling winnings.

## How can merchants stay compliant, ensure a smooth onboarding process, and efficiently fight fraud at the same time?

To stay compliant with regulations in your operating markets →

requires a strong in-house compliance and security team, as well as a partnership with a trusted, all-in-one verification provider that fights money laundering and fraud. Even one undetected case of fraud leads to fines unless you have robust verification policies and can prove that this specific case was just an exception within the margin of error.

To reduce pressure on the user, verification checks should be allocated throughout the player lifecycle and inserting them at the right time without hurting the onboarding process. For example, bank card verification and biometric checks can be asked after initial onboarding, at the first deposit stage, or even the withdrawal stage. Gaming companies should also think in advance about anticipated user traffic spikes ahead of major events like the Olympics or the FIFA World Cup. Sumsub created [an online calculator](#) to help betting platforms estimate potential fraud losses during major sports events in 2022.

### What role do international regulators play in fighting fraud in gambling? Would stronger regulations negatively impact customers' overall experience?

Almost all national AML regulations follow FATF recommendations, and AML/CFT requirements do not differ significantly from country to country. The main aspects of AML compliance will always be customer due diligence (CDD) procedures, risk assessment, ongoing monitoring, and suspicious activity reporting. Structured compliance regulation would help weed out unscrupulous players from the industry and protect users.

Otherwise, platforms with little or no KYC could expose clients to multiple risks. Users may lose their deposits and winnings. Even worse, their bank card or identity data may be compromised. Conversely, robust KYC procedures normally ensure that users experience no trouble with withdrawals and rest assured knowing their accounts are safe.

### How can merchants prevent online gambling fraud? What about PSPs?

Building effective KYC flows that effectively fight fraud and meet the full range of regulatory requirements is a big challenge for gaming platforms. Each platform must develop a programme in accordance with its gaming and market specifics. To stay ahead of the competition, it is vital to use the most advanced KYC/AML products on the market, such as transaction monitoring, or [KYT \(know-your-transaction\)](#).

With KYT, gambling companies can successfully manage risks by monitoring and reporting suspicious activities, analysing user behaviour, and cross-checking KYC data. Recently, Sumsub published its first KYC guide for gaming companies [in Europe](#) and in [North America](#), sharing detailed information on regulatory requirements and useful tips on how to build efficient user verification flow and keep onboarding rates high.

### Are there any types of online gambling fraud that you see trending next year? What should merchants pay attention to in the upcoming 12 months?

Fraudsters constantly invent new ways of illegal enrichment. In terms of actual fraud schemes that might trend in 2023, I would bet on the multi-accounting for bonus abuse. Multi-accounting is the creation of several profiles by one person within one platform. Depending on the company's requirements for data for registration, fraudsters can use a fake email or fake documents and third parties to get access to the account. Since gambling companies offer bonuses for new users, fraudsters exploit this through multi-accounting. This is both a direct loss through excess bonuses and an indirect one in the form of inefficient spending on marketing and promotion. Therefore, it's important to improve the data requirements for registration and ask for confirmation of the identity via technological solutions like Face Authentication.



[sumsub.com](https://sumsub.com)

**Sumsub** is an all-in-one verification platform that secures every step of the customer journey. With Sumsub's customisable KYC, KYB, KYT, and AML solutions, you can orchestrate your verification process, welcome more customers worldwide, speed up onboarding, reduce costs and steer clear of digital fraud. Sumsub achieves the highest [conversion rates](#) in the industry—91.64% in the US, 95.86% in the UK, and 90.98% in Brazil—while verifying users in less than 50 seconds on average. With over 2,000 clients across the fintech, crypto, transportation, trading, and gaming industries, Sumsub partners with Binance, Mercuryo, Bybit, Huobi, Unlimint, DiDi, Poppy, and TransferGo.

# Chargebacks 911

## Best Practices to Fight Ecommerce Fraud



**Monica Eaton** is the Founder of Chargebacks911 and Fi911. Monica has worked tirelessly to educate merchants and financial institutions about hidden threats in the rapidly changing payment fraud landscape, successfully protecting over 10 billion online transactions and recovering over USD 1 billion in chargeback fraud.

Monica Eaton ■ Founder ■ Chargebacks911

Fraud prevention should be a key concern for anyone who sells online. However, unlike other costs, fraud is preventable, and the figures show that companies can't afford to ignore it. Three-quarters of merchants reported increases in both fraud attempts and fraud rates by revenue in 2021, with the average cost of fraud management **increasing five-fold**. In 2019, ecommerce merchants spent an average of 2% of their annual revenue on fraud prevention. By 2021, that share had grown to 10%, while in 2022 **remained the same**.

The present article aims to explore the red flags you should look out for and share some best practices, given that fraud can happen at any time during the life of the transaction and it is increasingly prevalent 'post-transaction' via chargebacks.

### Red flags

Although there are new types of fraud being developed every day, they tend to have common features that can be used to identify a probable fraud attempt. The AI-enabled solutions that we will discuss later are designed to look for these signals and many others, but merchants can design their ecommerce solution to prevent these signs from becoming a possibility.

Some red flags to look out for include:

- **New email addresses:** Did a customer create a new or temporary ('burner') email address to make a purchase? This may be a sign that the buyer is planning to commit fraud, then disappear.
- **High-ticket value and velocity:** Fraudsters want to get the most value out of their efforts. To do this, they often buy high-value goods or use systems to push through large volumes of transactions or attempted transactions in bulk.
- **Expedited shipping:** Fraudsters tend to pick the fastest shipping

option – they have an interest in shortening the time during which they can be detected and get their hands on the goods.

- **Address mismatch:** The shipping address used by a fraudster will not match the billing address kept on file with the bank. While there can be good reason for this, often this is a significant warning of fraud.
- **Repeat IP addresses:** Although IP addresses can be hidden or spoofed, amateur fraudsters might use the same IP address for multiple transactions.
- **Chargebacks:** Most chargebacks you receive are cases of friendly fraud that originate with genuine cardholders. These claims can happen because of misunderstandings, or come from customers who erroneously believe a chargeback is a legitimate (or faster) way to resolve complaint. An increasing number of cases involve customers lying to get merchandise for free. To be effective, merchants need a dynamic, multi-level fraud management strategy that addresses pre- and post-transaction fraud.
- **Grooming your blacklist:** Fraudsters often escape typical blacklist strategies, opting for similar but not identical customer details. As a result, you could suffer repeated losses from the same criminal. The best way to spot this issue is to check your blacklist against your chargeback records. Maintaining a layered approach is the best method to uncover gaps in your rules or processes.
- **Realtime feedback:** Without data feedback – including refund results, any dispute prevention actions, and all chargeback data – your decision engine is operating without the most relevant information. Whether you can get access to this information in real-time or otherwise, is less important – just make sure you have access to all the data and are able to standardise relevant feedback. This will keep rules running as expected, taking action to block bad actors but not accidentally declining those who are good. →

## What to do about fraud?

When it comes to fraud, there are two divisions: pre-sale and post-sale. Pre-sale fraud prevention is best managed with fraud filters and strict policies, whereas post-sale or post-transaction fraud (chargebacks) requires a more tactical strategy to decision each chargeback. Optimum results are achieved when a retailer employs a competent solution for both.

### Deploy AI and machine learning

The most effective fraud prevention tools use artificial intelligence and machine learning to monitor, score, and make decisions about transactions. Keeping pace with the fast-evolving fraudster and learning in real time are crucial to good fraud prevention.

### Look for multiple data sources

You can integrate fraud signals from other data networks apart from your own, which will help you identify trends faster and be more in-tune with developing fraud threats and tactics. A good strategy is to leverage multiple data sources that can be contributed as enrichment data from other suppliers – such as chargeback management vendors. Chargeback management companies connect to post transaction data to enrich the transaction record and transmit this information for further processing.

### Authenticate buyers based on risk

Frequent shoppers with reliable and static address or geolocation data present lower risk than new customers with less reliable data, which means, in this case, friction should be introduced only when it is mandatory.

### Be PCI-compliant

PCI standards are meant to ensure that you're taking the necessary steps to protect consumers' personal data. PCI compliance protects your customers and insulates you against fraudulent purchases made using stolen data, as well as the PR backlash following a data breach.

### Train staff properly

You want your staff to be trained properly and to know the warning signs of fraudulent activity, especially when conducting manual reviews of transactions.

### Keep software up to date

Outdated fraud prevention solutions may fail to intercept new threats. Keep up with all software updates and patches and deploy them as soon as possible.

### Conduct regular audits

Don't simply assume that you're doing everything you need to protect yourself and your customers. Conduct regular audits of all internal operations and reviews of any fraud (or chargeback) losses you make to ensure you're learning lessons, making changes and doing what needs to be done.

### Using the right tools

Fraud prevention is about employing the best tools and strategies. Fraudsters spend 100% of their time on staying on top of their game – you should select the best tools and work with the best partners for your business to keep pace with their efforts. From customer onboarding screening to chargeback management and all steps in between, it is crucial to have a strategy for each.

### Defend chargeback losses and get educated

Many businesses accept chargebacks as a cost of doing business. Having the data, tools, and expertise to properly defend incoming chargebacks and recover your revenue is critical. Whether working alone or with a specialist partner, your ability to respond and manage this growing category is imperative.

[Click here for the company profile](#)



[chargebacks911.com](https://chargebacks911.com)

Founded in 2011, **Chargebacks911** is the first global company fully dedicated to mitigating chargebacks and eliminating chargeback fraud. As an industry-leading innovator, Chargebacks911 is credited with developing the most effective strategies for helping businesses manage disputes and reduce loss in various industries and sectors within the payments space.



# Fraud During the Holiday Season



As we are rapidly approaching the holiday season, our anti-fraud experts are keen on sharing the risks of businesses and end-users face during this busy time of the year. Efficiently fighting fraud and scams implies more in-depth consumer education, together with stronger customer authentication technologies provided by ecommerce platforms.

# Scott Augenbaum

## You Better Watch Out! You Better Not Click! – When Cybercriminals Want to Spoil the Holiday Season



**Scott** joined the Federal Bureau of Investigation (FBI) in the New York Field Office in 1988 as a support employee. In October 2003, Scott was promoted to Supervisory Special Agent in the Cyber Division, Cyber Crime Fraud Unit. Since retiring from the FBI in early 2018, Scott shares his knowledge by consulting with individuals, groups, and businesses of all sizes. If you are interested in booking Scott or learning more, you can reach out through his website or by writing to [wayne@waynehalper.com](mailto:wayne@waynehalper.com).

Scott Augenbaum ■ *Cybercrime Prevention Speaker & Retired FBI Supervisory Special Agent*

The holidays! You've got to love this time of the year.

It all begins with Thanksgiving – that time when we eat way too much turkey and pie, watch football and Macy's parades, all while avoiding heated political discussions with angry family members. However, as the holiday shopping season draws closer, Thanksgiving serves as a wake-up call.

Even before Thanksgiving, there are many deals you could take advantage of simply by shopping on your phone, but is there a catch? With the growing popularity of online shopping, stores are willing to push Cyber Monday closer to Thanksgiving Day. Moreover, Americans spend 95 million hours or roughly 3.5 hours per person, on average, browsing for treats and sales during Cyber Monday, which underlines the high stakes of the event.

### Cybercriminals don't celebrate Thanksgiving

But when they do, they're biting into turkey legs as they relentlessly prey on victims behind a computer screen. As we add items to our online carts, they are celebrating in a different way. This is the unfortunate time that might be referred to as 'Cybercrime Tuesday.'

### Stay ahead of a cybersecurity scandal on Tuesday morning

On Cybercriminal Tuesday, everyone receives an email that looks as if it was sent by Amazon, Best Buy, Target, Walmart, FedEx, UPS, or even the USPS, which may read: 'Your package has been delayed in shipping!' or 'Your item is out of stock!' or 'Your credit card is invalid'.

The email then directs you to click on a link, to log into your account and rectify the issue. Many gullible people click on it, which turns into millions of opportunities for a team of con artists to score a big payday.

### What happens when you click on the link?

1. You click on the link and get redirected to a phishing website, where you log in with your account credentials. At this time, the cybercriminal uses your account to max out your credit card and later sells the goods they purchased.
2. You click on the link and malware is installed on your device, which steals your username and password for all your sensitive accounts.
3. You click on the link and ransomware encrypts your entire home network and turns off all your smart devices - TVs, appliances, lights, cameras, and alarms until you pay the ransom, potentially impacting your privacy and the security of your loved ones.

### Expect (and suspect) all emails to be phishing emails

Cybercriminals are going to ramp up their efforts as we get closer to Christmas Day. So, even if you think that link is legit, do not click on it. Instead, log into your account from the browser and only get in touch with the customer service from the website you shopped, to avoid being scammed. →

## Cybersecure minds: Tips to make your holiday shopping more secure

Blue Christmas, White Christmas, Black Friday, Cyber Monday – we did it. We're now past Thanksgiving, ready for the shopping frenzy that comes with the kick-off to the holiday season.

If you are like most folks, you took advantage of some great deals online and stockpiled your gifts for family and friends. This is when cybercriminals start unraveling their plans for their next big payday. And, while we wait for our first wave of packages to arrive, they will start sending out their first wave of phishing emails.

### How can you be sure it's real or a hoax?

The first step is already done: you are aware that this could happen to you. You must also be sure to read your emails carefully and look at where the email is coming from.

Ten times out of ten, phishing emails will direct you to click on a link to resolve the problem when, in reality, you will be redirected to a false website (that looks incredibly similar to the original one), and asked for your credit card number, account number, or login information.

Avoid the hassle by going to the original website to log into your account. Nine times out of ten there will not be a problem at all.

### If it looks too good to be true, it probably is

While some deals are incredible, be wary of amazing price drops. Only shop at reputable retailers, directly from their website and not from your email, as it could be the difference between having your money stolen and having a happy holiday.

Do your research and be wary of fake websites. Fraudsters may even write fake reviews, trying to get you to believe you are getting the deal of a lifetime, so don't fall for it.

### The most important piece to any real or fake transaction is the money component

How do you pay for your purchases after ensuring the shopping link is secure? Which method is better – debit or credit cards?

You should only use your credit card for online transactions, not your debit card. A credit card is not attached to your bank account so you can later dispute a false transaction, in case you fear the fraudulent use of your credit card info.

However, when fraudulent charges are on your debit card, the money is removed from your checking account and you are then forced to work with the bank to have the funds redeposited in your account. You will need to file affidavits stating the charges are not yours and, in many cases, the banks require a police report. In some circumstances, it may take a couple of weeks to fix the problem, if it can even be resolved.

Remember your cybersecurity is in your hands. Don't let it get into the wrong ones! Happy shopping and happy holidays!

# CMSPI

With global online payment fraud projected to double between 2018 and 2023, we spoke to Domingo Figueira Orihuela, Ecommerce Consultant at CMSPI, to learn how the top European retailers are choosing the right fraud partners and holding them to account.



**Domingo Figueira Orihuela** is a consultant at CMSPI. He is specialised in ecommerce and works with merchants globally to drive additional revenue through optimisation of approval rates, the development of efficient SCA strategies, and balancing fraud through the optimisation of current fraud prevention mechanisms and the selection of the best solutions to fit each merchant's needs.

Domingo Figueira Orihuela ■ Consultant ■ CMSPI

## What does the European fraud landscape look like today?

Fraud is a constantly-changing area of focus for merchants –every day there's a new way of committing fraud that merchants must tackle. Friendly fraud, for example – where customers falsely claim they haven't received goods – became increasingly prevalent in the pandemic. We're also seeing more sophisticated types of account takeover (ATO) fraud in Europe, where a fraudster uses the customer's details to make payments.

These evolving types of fraud represent a huge concern for merchants because they're hard to detect. Fraud methods are constantly shifting, so merchants need to be proactively searching for solutions to protect them from every angle.

“ Whatever their anti-fraud strategy, merchants need to be in a strong position to challenge their partners – from cost terms to fraud rulesets and data accuracy – and use those insights to build a more productive setup for the long-run.

## Didn't SCA solve the problem?

Whilst SCA was intended to reduce fraud, we haven't seen significant evidence of SCA helping to limit fraud rates for our merchants.

Merchants who enforce 3D Secure on all transactions might have seen a low level of chargebacks, but that came at a price – often enough in the form of a hit to conversion rates and higher abandonment rates. Most merchants don't want to affect their customers during the checkout process, so they may have developed an exemption strategy that means assuming additional liability for chargebacks. So, regardless of SCA, there's always a balance between conversions, approvals, and fraud.

## How are merchants approaching the challenge?

There are many things merchants can do. First, to stay ahead of the curve, they need the best data possible about their customers. Merchants who have done that in-house might be limiting themselves to historic data on their own website, which may not even have flagged fraudulent transactions correctly. With newer types of fraud, being able to analyse a customer's recent behaviour with other retailers –biometrics, shopping patterns, and customer device information - can be very powerful.

We have also experienced a change in how merchants approach fraud screening. Now, we are seeing more and more merchants moving from post-authorisation to pre-authorisation screening. Previously, you would have someone manually reviewing a transaction before the goods were shipped. →

Now, you can obtain a decision in milliseconds, which you can later use to determine the best route for a transaction early in the process.

### Is there a one-size-fits-all approach?

The best option – post-auth or pre-auth, in-house or third-party – is going to depend on the merchant. For example, post-auth might make sense for verticals with a relatively long lead time between the transaction and the receipt of goods, like travel.

On the other hand, merchants with very short lead times, such as food delivery companies, might not be able to afford that delay and might prioritise having that fraud assessment conducted earlier on in the process.

The same goes for outsourcing - even if a merchant decides to use a third party, there are nuances. Ultimately, it comes down to the benefits of specialisation versus consolidation – acquirer-owned fraud rules can deliver some value, but dedicated fraud providers are now leveraging data from lots of merchants and have developed sophisticated machine learning algorithms to improve the accuracy and speed of their decisions.

It's an area where we are seeing innovation, and merchants at the top of their game are looking to utilise these useful insights. There are also optimisation opportunities regardless of which strategy you choose - in-house, acquirer, or third-party rulesets need to be constantly assessed based on the data you're seeing.

### What would be your message for merchants looking at their strategy today?

It's important to look at the impact of fraud holistically. It can be very easy to just focus on chargebacks as the only KPI relating to fraud. Even though it is one of the main KPIs, there are many other stages throughout the transaction process when fraud could be happening. Looking at it from a different perspective, merchants might have

a great fraud rate, but they are likely rejecting too many good transactions. Both being a victim of fraud and being repeatedly turned away when you have sufficient funds are negative experiences, and either one could mean losing a lifelong customer. Generally, we look at fraud from that authorisation perspective – are you getting too many declines through your fraud provider or legacy acquirer? Are your rulesets out-of-date? And how do you balance conversions and risk?

### Why do merchants need to act?

The main reason merchants need to act now is the customer experience. Imagine your credentials being used to make a fraudulent payment – the need to go and resolve that with your bank would likely make you never want to shop with that merchant again.

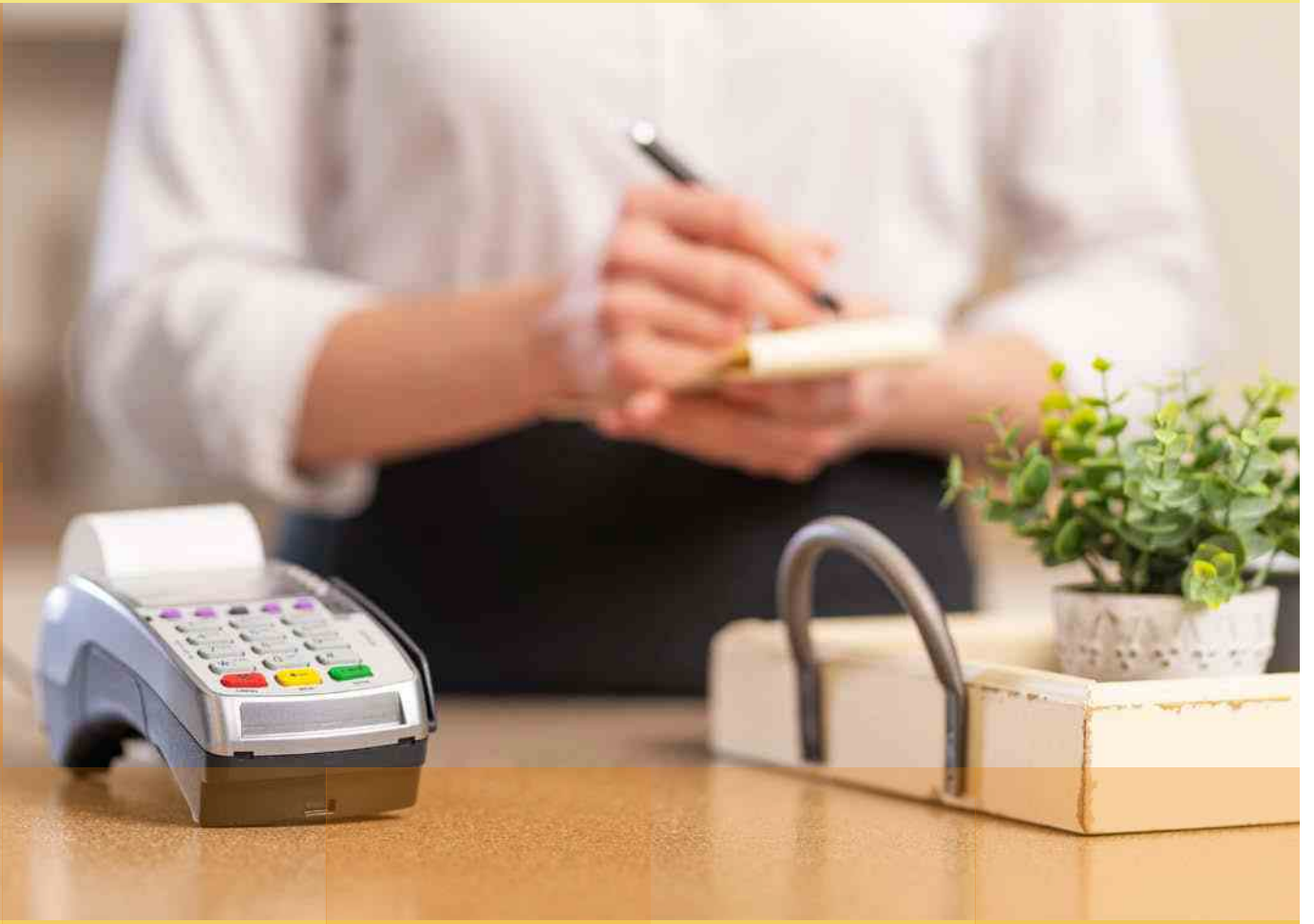
This could prove a concern, especially with the newer types of fraud, which require a holistic view of customer behaviour, such as login attempts and similar transactions with different merchants. But it's also about your top line: roughly, CMSPI estimates that European merchants lost EUR 40 billion to falsely declined transactions in 2021 alone. Whatever their anti-fraud strategy, merchants need to be in a strong position to challenge their partners – from cost terms to fraud rulesets, to data accuracy – and use those insights to build a more productive setup for the long run.



[cmspi.com](https://cmspi.com)

At **CMSPI**, our payments experts provide advisory services and powerful analytics. Our ultimate goal? Supporting a more innovative and productive payments ecosystem. For hundreds of clients across the globe, our insights help improve performance and create positive change.

# Best Practices for Fighting Fraud – Brief Q&A Session



- [Wargaming.net](http://Wargaming.net)
- Augie Kennady



**Elena Emelyanova**

*Senior Payments and Fraud  
Manager*

Wargaming.net



## Which fraud trends did you see on the rise in the past 12 months?

Wargaming is definitely one of those gaming companies that is lucky enough to have a stable variety of fraudulent activities appearing on a yearly basis. The year of 2022 was not an exception, bringing us lots of interesting and mind-blowing cases to fight with.

Wargaming's main fraud influencer of this year was account takeover (ATO). It may sound quite ordinary, especially since this type of fraud was never a 'headache' for us. However, we saw a peak of activity from the mid of the year, specifically in the European region.

The other trend we see is related to Gifting – the area we were almost sure is under our full control. I must admit that our fraudsters are definitely creative. They need to be extremely inventive to do their job properly.

## Will the current global economic context and the latest regulations, including for crypto assets, affect the level of fraud?

I do believe that every new technology or regulation, regardless of whether it was designed specifically to prevent fraud or not, is, in the end, serving yet another impulse for fraud to appear or to be pushed to somebody else. Global fraud levels will doubtfully be impacted. However, there will be industries which will catch the fraud ball due to the impact of global economic changes and the latest regulations.

Gaming is an industry married to fraud, thus, no matter what, there will be always a struggle with bad guys at some level, which means we are not even close to bringing the fraud level to its minimum.

## Which tools do you consider the most effective into keeping fraudsters away, without adding extra pressure on legit consumers?

The most effective tool would be the combination of multiple technologies and practices existing in a market. However, even in such case, the used tools will not be efficient forever. Ecommerce is a rapidly developing environment, including its fraud component. Thus, the efficient tool would need to be flexible and adaptable.

A combination of Machine Learning, Adjustable Fraud rules, and Manual monitoring could prove effective, although quite expensive. That's why, in most of the cases, you will see companies opting for only one component of the solution above.

# Augie Kennady



**Augie Kennady**

*Director of Trust & Safety*

*Chegg*

## Which fraud trends did you see on the rise in the past 12 months?

The reality is that fraud adapts to however you combat it. All over the world, you'll see similar card testing schemes, stolen-card purchases, and Account Takeover — anything that gives users an 'in' to your product. The behavioural patterns present analogously to dipping a toe into a cold pool — the fraudster tests a new tactic or pattern and then gradually expands it, as the level of comfort and confidence grows. Catching the signals early is paramount.

## Will the current global economic context and the latest regulations, including for crypto assets, affect the level of fraud?

The impact of both factors depends on the offerings of a particular company. A company that permits only domestic sales is unlikely to experience the impact of abuse that a more global company may encounter.

There is an important point to keep in mind here — while macro-economic conditions are generally favourable to fraud, fraud isn't a game fought on the macro-stage. It is a game fought on a firm-level. It's the age-old adage: 'You don't need to outrun the bear; you just need to outrun the other campers.'

At the end of the day, threat actors want to make money. If they have three comparable financial opportunities, but one of those opportunities is more sophisticated in their abuse prevention, the threat actor is likely to focus on the two less-sophisticated platforms. That's why every company — no matter the platform, product, or approach — should understand what they can do to mitigate abuse.

## Which tools do you consider the most effective into keeping fraudsters away, without adding extra pressure on legit consumers?

Understand your platform. Where are the moments of greatest risk? Is it at login? Is it at order placement? Content or product access? Account access? Wherever the greatest risk may reside, you should find a partner who will be able to implement their technology at that level. Moreover, ensure that the partner allows for custom business rules. No two businesses are identical.

What worked marvellously for some companies may prove unsuccessful for your company. Strong threat-defence partners understand that their clients — the firms themselves — are collaborators in their model. Firms seeking guidance should immediately assess potential collaborators' ability of implementing custom logic.



# Latest Updates on Technology That Helps the Industry Detect and Prevent Fraud



An important part of keeping the payments process safe is deploying the latest technologies to better identify, prevent, or fight fraud before causing damage. Our industry experts have laid down the best practices in fraud decisioning, orchestration, and tokenization to effectively deter fraud in ecommerce, without compromising on user experience.

# Nethone

We sat down with Maciej Pitucha, Chief Data Officer at Nethone, and talked about how fraud prevention can positively influence a customer's journey and, at the same time, help merchants differentiate between legitimate users and bots for enhanced customer services.



**Maciej** is an experienced manager focusing on building data products. His vast experience covers actuarial science, data science, data and software engineering. Before joining Nethone in 2018, he worked at Deloitte and EY delivering advisory services for insurers in the EU (risk and actuarial). At Nethone, initially, as the Head of Data Science, is responsible for delivering the best-modularized fraud prevention and risk detection platform to Nethone's global customers. Maciej holds a Master's degree in Quantitative Methods in Economics & Information Systems from the Warsaw School of Economics (SGH).

Maciej Pitucha ■ Chief Data Officer ■ Nethone

Before we dig into fraud prevention strategies, could you please present the main stages of the user life cycle during a consumer's journey?

As part of our fraud prevention efforts, we monitor and check four user journey stages. The first step regards user acquisition, where consumers get in touch with the product, service, or brand. For us, it's relevant to know the interaction channel – browser or mobile (Android and iOS) – and the users' true intentions. We usually detect high levels of bot activity at this stage.

“ The synergies between our products enable us to detect risks, offer end-to-end protection, and provide risk-based KYC in the same solution.

The second step is 'login and registration', meaning the user has entered their details (name, address, email, etc.) and is ready to start shopping. Recurrent user logins are also checked for fraud. After this, the customer completes the transaction through the checkout process. In several instances, the fourth stage occurs when consumers initiate transaction disputes asking for refunds.

What problems can online consumers encounter during each stage of the end-user life cycle?

The issues that are most likely to arise are related to fraud and UX. A cumbersome authentication process can alter or stop the buying journey and make consumers take their business elsewhere. So, there is a hassle for the consumers, but also a loss for the merchant. The image below illustrates the most prevalent types of fraud that can occur at each stage in the user life cycle. Some of them, such as account takeover (ATO), identity fraud, or synthetic ID fraud, primarily affect the end user.

How do these problems affect ecommerce merchants?

Consequently, the problems above also affect merchants. Moreover, ecommerce businesses are also faced with affiliate fraud, ATO, promo and policy abuse, return fraud, and first-party misuse. These types of fraud are common in the industry, so we are not dealing with a new phenomenon, but rather with a persistent one that carries severe consequences beyond friction and false positives. →

Besides revenue loss, ATO can lead to a damaged brand reputation. Promo and policy abuse can force merchants to tighten the rules, thus, discouraging loyal customers from shopping with them. Chargebacks and first-party misuse are not only about paying fees associated with disputes, but about being subjected to card schemes monitoring programmes that come with hefty penalties.

### How can we address business' needs along the user life cycle related to fraud and risk?

Our presence at every step of the user journey enables us to address each type of fraud along the way. Thanks to a modularised approach, we are also flexible enough to meet specific challenges that ecommerce businesses fight with. For example, ecommerce merchants can take advantage of SCA-related exemptions to optimise their payment processing setup, resulting in higher conversions – if we determine a transaction is safe, 3DS is not required.

Moreover, to spare merchants from dealing with chargebacks, we activate our early chargeback notification alerts (powered by third-party providers); if we detect fraud, the transaction is simply rejected, and in case of legit requests, merchants can quickly refund the consumer, so no dispute is necessary.

The synergies between our products enable us to detect risks, offer end-to-end protection, and provide risk-based KYC in the same solution. Any business that requires thorough ID verification of their users can encompass fraud detection, KYC, and AML, under one API. In response to the risk assessment that we undertake, the user is guided to either a hard or a soft check. The key benefit we're offering here is that the journey stops when fraud is detected. For instance, in the case of bot detection, we don't recommend further KYC checks, thus saving time and money for our clients.

### What role does behavioural biometrics play in solving these issues?

Behavioural biometrics keep the balance between user convenience and protection. Device movements are analysed in the background, and we can detect anomalies and bot activities in real time. Yet, the most valuable aspect is determining where the suspicious behaviour comes from, so one can proactively act on any attack targeting their business. Our intelligence team frequently explores the dark web to discover new signs of fraud based on behavioural biometrics. Fraud can be sophisticated, but is also characterised by cheap and unskilled labour, such as click farms.

### Could we conclude that a modularised fraud prevention solution makes the customer journey a positive experience? Will this theme become a trend in fraud prevention in 2023?

Apart from the flexibility that it offers to businesses looking to employ just one or multiple parts of the entire product, a modularised approach is, indeed, capable of customising the user journey through a fast and safe path toward the checkout.

The trend is dictated by more and more companies embracing this model, but we aim to stand out from the current reality by offering a 'try-it-for-free-and-onboard-yourself' tool. This will allow anyone interested to enrol in a free trial that walks them through the product's main features so they can have an accurate picture of how it works and how it can benefit their specific needs and challenges.

[Click here for the company profile](#)

**Nethone**

[nethone.com](https://nethone.com)

**Nethone** is a machine learning-based fraud prevention SaaS company that enables ecommerce merchants and financial institutions to holistically understand their end-users – also referred to as Know Your Users (KYU). With our proprietary online user profiling and AI-powered tools, we can block all risky users without friction to the good ones by exhaustively screening every single one.

# Ping Identity

We talked to **Maya Ogranovitch Scott**, Solution Marketing Manager at Ping Identity, about fraud orchestration and the best practices in fraud decisioning that can help end-users stay safe while enjoying the perks of a strong digital identity when shopping online.



**Maya Ogranovitch Scott** is a Solution Marketing Manager for Ping's fraud prevention solutions. She is passionate about leveraging the power of identity to help enterprises deliver exceptional customer experiences that are simultaneously secure and seamless.

Maya Ogranovitch Scott ■ Solution Marketing Manager ■ Ping Identity

With fraud on the rise globally as an unwanted effect of the drive of ecommerce, what is the impact of fraud on merchants and end-consumers globally? Could you elaborate a little on the US market?

Even now, with most pandemic restrictions lifted, many shoppers won't return to stores for purchases they once made in person, having become accustomed to the convenience of online shopping.

*“ Make sure to create strong, unique passwords when required, and opt for biometric authentication when it's available. Keep good track of all financial accounts and watch for unusual activity.*

Fraudsters are taking advantage of this, and the cost of fraud continues to grow. **The global cost of ecommerce payment fraud alone was USD 20 billion in 2021, an increase of over 14% year over year.**

**In the United States, consumers reported losing USD 5.8 billion to fraud in 2021, an increase of 70% year over year.** While this concerning growth includes all types of fraud, ecommerce losses make up a portion of that number. And, of course, when it comes to ecommerce fraud, merchants are often the ones left responsible for the cost of resolution, making these trends very concerning.

What are the main types of fraud merchants face? Is the cost of fraud largely due to fraudulent transactions, or are there other types of attacks that happen at other stages in the user journey?

Payment fraud is still the biggest pain point for most merchants, but it is far from the only type of attack that merchants need to defend against.

Fraudsters may take over accounts to steal PII or even loyalty points, which may be worth real, measurable money, as in the case of airline miles. They can abuse sign-up bonuses or affiliate rewards by deploying bots to create dozens of new accounts or simulate clicks and impressions. The fact is fraudsters can do a lot of damage long before they get to the 'buy' button – and the goal of merchants should be to spot and stop them before they get there. The good news is that detecting and mitigating fraudulent sessions earlier will also have the effect of reducing payment fraud.

What are fraud decisioning and orchestration, and how can they change the way merchants respond to fraud?

Fraud decisioning tools allow fraud teams to set up automated, effective fraud mitigation. Within these tools, fraud teams can define the logic that determines the risk levels that will trigger mitigation and the types of mitigation measures that are appropriate for different types of situations.

These tools can take multiple sources of fraud signals into account, leading to greater detection accuracy and more targeted mitigation.

→

Meanwhile, orchestration brings together a variety of tools to create user experiences that feel seamless and easy from the customer's perspective, even when many systems are at work behind the scenes.

Well-orchestrated customer journeys allow for many branching paths, with users sent down the appropriate one, based on their circumstances and characteristics. This includes paths reserved for suspicious users that can help greatly reduce fraud.

### Can orchestration help control the customer experience aspect of fraud prevention more effectively?

This is arguably orchestration's greatest strength. Customer experience and fraud prevention can be inversely related, but with well-orchestrated customer journeys, this doesn't have to be true. Orchestration can bring together the various tools used for fraud prevention and embed them more naturally within the user journey.

Based on the information coming in from fraud detection tools and the risk evaluation delivered by decisioning tools, a legitimate user with good intent can still have a frictionless experience and transact with ease, because only risky users experience the hurdles associated with extra security steps. Further, a merchant can present fraud controls earlier in the session when they are needed, instead of putting multiple security steps right before the checkout, when the likelihood of cart abandonment is higher.

### What tools enable merchants to get fewer false positives?

The best approach involves multiple layers of protection deployed across the entire user session. Detection tools that look at user characteristics and behaviour can help get a clearer picture of user intent. Ultimately, examining more information will automatically lead to more accurate decisions. Merchants need to adopt a session-centric approach to fraud detection, analysing user behaviour from the moment the user first begins interacting with one of their digital properties, whether that user chooses to log in or to proceed as a guest.

Fraud decisioning should then take into account all of the available contexts to challenge suspicious users when appropriate.

### How does a merchant's fraud prevention strategy boost UX? How can end consumers improve their online behaviours to deter fraudsters?

To boost UX without loosening fraud controls, merchants should move away from high-friction active fraud checks such as CAPTCHA, to effective passive checks instead. Ideally, a good tool should be able to determine the difference between a bot and a human without forcing the user to squint at tiny, illegible text on their mobile screen. Passive checks can also help organisations get to a good level of certainty about user intent. Active checks should come after and be applied only to sessions that are already exhibiting some level of risk.

This is where multi-factor authentication (MFA) can be really useful. It is a softer mitigation method that helps an organisation gain confidence in a customer's identity. It is also generally easy for legitimate customers. Meanwhile, fraudsters often don't have the time or inclination to break through the second layer of defence.

As for the advice end customers should consider, enabling MFA is always a great step in protecting online accounts. Make sure to create strong, unique passwords when required and opt for biometric authentication when it's available. Limit social media sharing of personal information that can be used to answer security questions. Keep good track of all financial accounts and watch for unusual activity. All these pieces of advice can help individual consumers to protect themselves, but, ultimately, merchants must remain watchful as well.

[Click here for the company profile](#)



[pingidentity.com](https://pingidentity.com)

At **Ping Identity**, we believe in making enterprise experiences both secure and seamless for all users, without compromise. That's digital freedom. To achieve this, the PingOne Cloud Platform turns you into an experienced artist who can bring exceptional journeys to life with a simple no-code canvas. You can deliver password-less authentication, protect user privacy, prevent fraud, architect for zero trust, and much more. For more information, please visit [www.pingidentity.com](https://www.pingidentity.com).

# Juniper Research

## Tokenization and the Fight Against Fraud



**Nick Maynard** is Head of Research at Juniper Research. His key area of focus is the fintech & payments area, including embedded finance, Open Banking, and digital wallets, among others.

Nick Maynard ■ *Head of Research* ■ Juniper Research

Protecting customer payment data is integral to the security and success of the payments ecosystem. In an increasingly interconnected world, with a growing number of payment options, the need for strong security solutions is clear, with fraud being an ever-present danger. Payments currently fall under four main categories: card present transactions, ecommerce, mobile payments, and IoT payments. With so many different payment methods now in use, the need to ensure that consumer data is protected across all channels is only growing and will continue to do so, as more markets further digitise payments.

### How tokenization works

The process of tokenization is not a new concept and is where something with high value (e.g., debit or credit card account numbers) is replaced by something with low or no intrinsic value. Therefore, payment tokenization enhances transaction security by removing the most valuable data from malicious actors from the transaction. In the context of mobile payments, EMVCo defined the first standards for tokenization back in March 2014.

Under the first version (v1.0) of EMV's tokenization framework, payment tokens are used to replace the PAN (Personal Account Number) in payment transactions, whereas non-payment tokens may be used for ancillary processes, including loyalty and tracking. Occasionally, the last four digits of the PAN may not be encrypted for these processes, including customer service, loyalty tracking, digital wallet display, and receipt creation.

Based upon the EMV specification, a static token is combined with a dynamic component, specifically a uniquely generated cryptogram, for greater security. EMVCo further expanded upon these capabilities in v2.0 to include both mobile payments and ecommerce, while adding the ability to share tokens between merchants. Since then, EMVCo has further updated the framework, with v2.3 being released in October 2021. This latest update offered further information on the technical aspects of token creation to provide greater clarity over when and how payment tokens are generated.

Tokenization is frequently adopted to reduce the scope of the PCI DSS (Payment Card Industry Data Security Standard) as set out by the PCI SSC (Payment Card Industry Security Standards Council). This is because payment tokens are inherently not payment information, and, as such, they do not fall under the umbrella of PCI DSS requirements outlining the secure transmission of payment data. However, it is important to note that even with tokenization in place, merchants must still meet the rest of the compliance requirements.

### Tokenization central to fighting fraud

The rise of tokenization comes at a time when online payment fraud is increasing, with Juniper Research forecasts showing the total cost of ecommerce fraud to merchants will exceed USD 48 billion globally in 2023, from just over USD 41 billion in 2022. →

With the rise of alternative payment methods creating new and varied risks for payment fraud, doing the best to prevent payment fraud and increase the security of transactions has never been as important.

This is where tokenization comes in: a major source of fraud is where payment details are exposed in data breaches, then these stolen details are used to make fraudulent purchases. However, under a tokenized model, the data breach cannot expose what it does not have, namely, the full payment details. Reducing the data being transmitted to a token means that this, if exposed, is useless to fraudsters.

By taking this simple step, payments can offer greater security and reduce one of the biggest risks of data breaches. While this will not eliminate fraud entirely, it will have a significant impact, securing the overall customer journey.

### The future of tokenization

Given the strong benefits of tokenization, its future trajectory is upwards. Our most recent study found that the total number of tokenized payment transactions will exceed 1 trillion globally by 2026, rising from 680 billion in 2022.

Figure 1: Global Tokenized Transactions (mln) 2022 & 2026

Much of this growth will be related to the rise of 'one-click' solutions, such as click-to-pay, that use card-on-file tokenization to store a customer's payment credentials, enabling them to auto-fill their checkout details and complete transactions via a single click.

However, tokenization is not limited to just existing use cases. IoT payments, for example, are a great area where tokenization can have a major impact. We forecast that tokenized IoT transactions will reach 19 billion by 2027, growing 400% from just 3.8 billion in 2022. At a basic level, tokenization is fundamental to facilitating IoT payments; enabling transactions to be made via new use cases and form factors, unlocking new revenue opportunities for payment providers.

However, tokenization is highly competitive, with lots of card payment networks and third-party providers offering capabilities in this market. Tokenization is also not restricted to just one type, with different types including network and PCI tokenization, meaning that there are options for tokenization vendors to compete on going forward, as well as exploring the area of the IoT.

Source: Juniper Research



[juniperresearch.com](http://juniperresearch.com)

Juniper Research specialises in providing best-in-class market research across mobile, online, and disruptive technologies. We offer in-depth reports, forecasts, annual subscriptions, and consultancy. Our global clients include banks, payment providers, and many others. To find out how we can help you, contact [info@juniperresearch.com](mailto:info@juniperresearch.com) or visit [www.juniperresearch.com](http://www.juniperresearch.com).

# Operations and Costs



With fraud on the rise globally, businesses must rethink their budgets to include a higher focus on their fraud prevention teams, even in times of economic downturn. This chapter explores the tactics that promise the most when it comes to facing uncertainty in the coming year.



# ACI Worldwide

We talked to Amanda Mickleburgh, Director, Merchant Fraud Product at ACI Worldwide, about proofing the fraud prevention solutions merchants can opt for to stay ahead of fraudsters in these difficult economic times.



**Amanda Mickleburgh** has held a variety of strategic roles since joining ACI Worldwide in 2007, with a strong focus on ecommerce fraud prevention. Specifically, she has developed expertise in leveraging data intelligence to aide checkout conversion and remove friction from payment flows. Amanda also joined the Merchant Risk Council (MRC) European Advisory Board in 2021 and, more recently, she has been appointed Co-Chair, deepening collaborations with industry experts.

Amanda Mickleburgh ■ Director, Merchant Fraud Product ■ ACI Worldwide

## What is the impact of the economic downturn on threats and fraud?

Fraudsters have been quick to exploit the current cost-of-living crisis for their own gain, adapting threat tactics and targeting the vulnerable. Consumers are increasingly cost and discount driven, making them more likely to buy from 'cheaper' unfamiliar websites, foreign marketplaces, or shady links where they may be at higher risk of fraud, fake goods, or ID theft.

“ To shift the decision lens from fraud detection to fraud prevention, management must rethink its value for the entire business and recognise providers as strategic growth partners.

However, consumers can be both the bad actors and the victims. Economic pressure can tempt them to abuse return, refund, and chargeback policies, so we can expect tougher safeguards to help tackle this. Visa, for example, has changed its requirements for how much and the types of evidence a business must submit to resolve customer disputes pre-chargeback, and we're expecting other businesses to adopt similar policies.

## What are the top fraud trends to watch in 2023?

### The cost of fraud is likely to increase even further

Cybercriminals continue to attack a wider set of payment methods, including contactless, mobile apps, and digital wallets. Every fraudulent transaction now costs **3.75** times the lost transaction value – 19.8% higher than pre-COVID-19. ACI's response tools aim to improve fraud detection and respond quickly to fraud attacks. Our incremental learning solution, self-learning models, not only help to improve fraud detection, by up to 85%, but can also reduce fraud losses by up to 75%.

### Fraud will become even more diverse, sophisticated, and targeted

Our own data shows a ramping up of synthetic fraud threats fuelled by BOT attacks, phishing scams, and account takeovers. Identity fraud continues to be an issue. We are also seeing a significant increase in the average ticket value of friendly fraud, which indicates that fraudsters are targeting high-value items like electronics and travel.

### Attitudes to fraud prevention will shift as it gains ground as a revenue booster

Stakeholders are waking up to the fact that there are advantages to be gained beyond mitigating risk and protecting against reputational damage. Today's advanced real-time fraud management solutions can be integrated within the payments flow, helping them to cut fraud, reduce expensive chargebacks, and minimise false declines – all of which positively impacts a merchant's bottom line and growth. →

## As global website traffic is going down, so does the growth of ecommerce. How can merchants increase ecommerce conversion while mitigating the current economic impact?

When evaluating vendors and solutions, decision makers should focus on customer experience, as well as ROI. Advanced fraud management with smart decision engines can help avoid cart abandonment by reducing false positives and checkout friction to provide more seamless shopping experiences.

As customers feel the pinch from rising inflation and economic recession, they're demanding more streamlining and efficiency in the way they pay for goods and services, how they are delivered, and how they are rewarded. Merchants can encourage greater acquisition and conversion by offering more flexible payment methods, home delivery options, and loyalty programmes. But they need to do this without opening the door to more fraudsters, for example, by expanding the fraud detection's role to encompass a broader range of use cases like promotional, reseller, and loyalty programmes.

## How can management be made to see the true value of investing in the latest fraud prevention technology from a third-party provider?

To shift the decision lens from fraud detection to fraud prevention, management must rethink its value for the entire business and recognise providers as strategic growth partners. End-to-end fraud management improves merchants' core business without taking its eyes off selling, by helping to address key challenges around conversion, operational efficiency, and resource management.

Advanced fraud prevention technology and orchestration, integrated directly into the payment flow, ensures operations are scalable, fit for growth, and more able to support national and international expansion with geo-compliance. It provides easier and more accurate fraud detection, real-time decisioning, and strong payment

intelligence analytics, so merchants can make better decisions, take greater control of costs, and deliver smoother experiences.

Above all, it can do this without putting excessive pressure on existing resources by using automated tools, intuitive customisation, and consolidated dashboards. Fraud prevention providers can also help to tackle talent shortages, acting as an extension to internal teams and providing additional technical knowledge, as well as sector and geo expertise.

## Lastly, do you have some practical tips for the fraud team who need to cope with tighter budgets and smaller teams?

Manual processes are time consuming and costly. Take a closer look at workflows and see where you can increase automation for faster response time and more efficient decisioning.

Leverage advanced technology like sophisticated machine learning (ML) that learns automatically in real-time without retraining. It reduces operational burden and responds to changing patterns and behaviours immediately. In production, ACI incremental learning has been shown to outperform traditional ML by 15%.

Remember experienced providers like ACI have global payments risk optimisation teams that can provide much needed support and talent – lean on these to plug gaps in your capability and help make platforms and processes more efficient.

[Click here for the company profile](#)



[aciworldwide.com](https://aciworldwide.com)

**ACI Worldwide** is a global leader in mission-critical, real-time payments software. Our proven, secure, and scalable software solutions enable leading corporations, fintechs, and financial disruptors to process and manage digital payments, power omnichannel payments, present and process bill payments, and manage fraud and risk. We combine our global footprint with a local presence to drive the real-time digital transformation of payments and commerce.

# CAF

## Why Ecommerce Is More Vulnerable to Fraud During Economic Restrains



**Darryl Green**, CEO of CAF, is an experienced entrepreneur in the global identity and fraud prevention market. He was a Co-Founder at Ethoca and helped build and establish the company as an industry leader in collaborative fraud loss prevention.

Darryl Green ■ CEO ■ CAF

The booming ecommerce sector is on a high-growth path with no slowdowns in sight any time soon. If estimates are anything to go by, the ecommerce sector may reach **USD 8.1 trillion by 2026**.

Low barriers to entry, multiple digital payment options, ease of use, and the ability to make device-agnostic purchases are driving the prolific growth of ecommerce platforms around the world. A growing global customer base is also driving cross-border ecommerce, as consumers look for better deals and businesses try to expand their operations across diverse geographical locations. The global B2C cross-border ecommerce is expected to clock **USD 5,576.73 billion in revenues by 2030**.

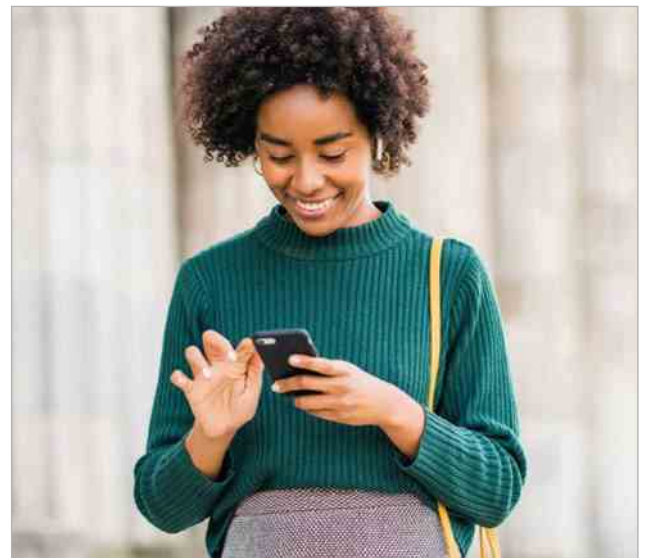
Unfortunately, the reasons behind this prolific growth are also the reasons that make the ecommerce sector – both domestic and cross-border – susceptible to fraud.

### Growing fraud in the ecommerce sector

As new ecommerce players emerge and compete among themselves to acquire customers, they are trading off verification for improved user experience, allowing users to register with little or no information. They are also introducing new sales channels and digital payment methods to facilitate online shopping for their consumers. However, fraudsters exploit these conveniences for new account fraud, account takeover, payment fraud, and a host of other criminal activities.

Fraudsters can use these fake and compromised accounts to impersonate sellers and post ads of non-existent items to dupe users into paying for goods that would never get delivered. Posing as buyers, they can use stolen credit card details to make purchases

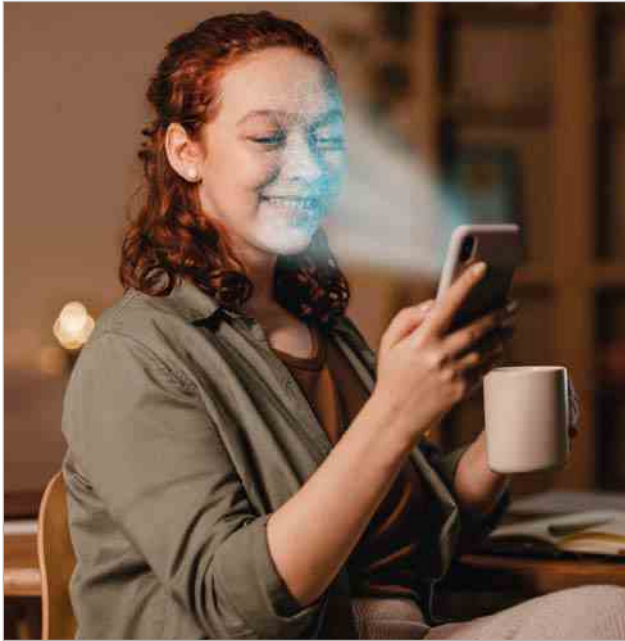
or hoard inventories. They may tarnish the image of genuine buyers by manipulating the reviews and ratings of their products through fake negative reviews and lower product ratings. Even worse, they can launch phishing campaigns to trick users into sharing their personal and financial details.



### Why fighting fraud should be a priority for ecommerce platforms

The problems for ecommerce platforms can snowball into a disaster if these fraudsters are left unchecked. Not only do ecommerce platforms run the risk of financial losses due to fraudulent activities, but they also disrupt user journeys and cause consumer resentment. Unhappy users may choose to avail of a competitor's platform leading to loss of revenue and brand reputation to the affected platform. Therefore, ecommerce players need to build trustworthy platforms where both buyers and sellers can transact in a safe and secure digital environment. →

Trust is the cornerstone of an ecommerce platform, especially because neither the sellers nor the buyers know each other. They trust the ecommerce provider for providing them with a safe and secure platform for transactions. It is, therefore, the responsibility of the ecommerce players to ensure secure transactions through robust user verification methods that allow balancing fraud prevention with a superior user experience.



### Step up your fraud prevention measures

Ecommerce is the brightest star of the digital economy, which is abuzz with activity 24/7. Ecommerce players cannot allow fraudsters to exploit this global ecosystem for monetary gains or consumer abuse. They need to step up their fight against fraudsters with robust fraud prevention solutions that help identify fraudsters from authentic users. For this, they need verification mechanisms that not only address the authentication challenges but also help maintain the user experience that consumers globally expect.

Ecommerce platforms often verify their users based on the documents and proofs that users submit. Fraudsters can use stolen information or create fake documents to pass these verifications. Therefore, it is essential that ecommerce platforms ascertain the authenticity of the information and the documents by checking them on several parameters before allowing the user to proceed any further.

However, in a digital-first economy, manual review is not a sustainable solution, as modern digital businesses must approve or reject user requests in near real-time. Consumers expect their requests to be processed instantly, whereas manual reviews take time to process as they involve massive human effort. Further, manual reviews are prone to human errors and bias.

Ecommerce platforms need automated verification solutions that leverage the power of the latest technologies – such as optical character recognition, artificial intelligence, machine learning, facial authentication, behavioural biometrics, proof-of-life, liveness, and MFA – combined with a touch of human expertise. This combination of technology with a hint of the human element can enable them to accurately detect and stop fraudsters early in their attacks, while also preserving an excellent user experience.

Collaboration and sharing intelligence can become crucial weapons in the fight against fraud. Each member can benefit from the insights on new fraud tactics detected anywhere in the network and prepare in advance to fight off evolving threats. Ecommerce players that leverage threat intelligence to take proactive fraud prevention measures stand to gain an edge in this fiercely competitive market.

[Click here for the company profile](#)



[en.caf.io](https://en.caf.io)

CAF is a leading provider of end-to-end identity verification, proofing, and authentication solutions, that combine advanced computer vision ML models, an AI-powered decisions engine, and sophisticated identity orchestration with an extensive collection of biometrics and identity databases.

# Standards and Compliance



To ensure a high level of security, merchants must go to extreme lengths and provide strong customer authentication without too much friction for the end-user. One way to help merchants maintain low abandonment cart rates and provide maximum user satisfaction is by implementing the latest standards and regulations, including PSD2, with its SCA requirements, and keeping an eye out for PSD3. This chapter focuses on the ever-changing field of anti-fraud regulation and provides the latest updates with valuable input from our industry leaders.

# Worldline

## How to Optimise User Experience While Ensuring a High Level of Security



**Claire** is responsible for the product management of Strong Customer Authentication & Security solutions such as Access Control Server, Trusted Authentication, and Digital Intrusion Protection. With 10 years of experience in international business developments and bids, she has developed strong skills to understand customers and market requirements, with a special focus on security, payments, and identity.

**Claire Deprez-Pipon** ■ *Lead Product Manager of Identity & Authentication* ■ Worldline

Strong authentication has been deployed since June 2021. It was intended to promote innovation and fight against fraud in online card payments. Indeed, in 2019, **80% of the value of card fraud resulted** from Card-not-present (CNP) transactions.

The primary objective of reducing fraud was achieved, as a significant decrease in CNP fraud can be seen; for remote card payments reported by acquirers, the share of fraud in total volume is five times higher for the payments authenticated without SCA compared with **the payments authenticated with SCA**.

Moreover, even if the kick-off has been complicated for many e-retailers, success rates on strong authentication have also increased. A new authentication method implemented will have an increase in the success rate of 30% in the first six months of the implementation, mainly due to:

- Enrolment time of the authentication method;
- Time for cardholders to learn how to use the authentication method;
- Time to deal with any problems integrating the payment method into the end-to-end purchase process;
- Communication to support the cardholder in enrolment and authentication.

### What can be done to make the user journey smoother?

The reinforced One-Time Password SMS (OTP) has often been deployed as a complement to a mobile strong authentication method, because it is simpler to implement, and allows it to meet time constraints. However, it is a less secure method (the SMS is not encrypted, the message can be intercepted; the OTP and the password are privileged factors for phishing because they are easily

transmitted, etc), and whose ergonomics are not the most suitable (password can be forgotten, two-step strong authentication, etc).

To remove friction from the user journey, banks must:

#### 1. Use an authentication method that does not impact the user experience

- Implement a transparent authentication factor, based on the trusted device (a smartphone or browser). This authentication method is a good alternative to SMS OTP, as it eliminates an authentication step thanks to the possession factor which is transparent while providing a higher level of security.
- Implement a biometric solution, whether linked to the OS (smartphone biometrics, computer biometrics), or via external solutions. This technology is preferred by many users as it improves the overall experience with password-less authentication (**74% of respondents chose biometric authentication as their preferred method**). The use of biometrics can increase the success rate by at least 10%.

#### 2. Work on the authentication workflow and user journey

The integration of an authentication method into the user journey can impact the success rate. The diversity of the type of integration is multiplied at each node of the authentication and payment chain.

The same authentication method can be integrated in different ways in the banking environment (Software Development Kit, separate mobile application, authentication flow, PIN, or biometrics). Moreover, authentication pages are integrated by merchants differently, depending on the channel (mobile, browser) or the type of integration (i-frame, redirection, 3DS SDK). →

Therefore, it is important to implement the ergonomic evolutions proposed by the EMVCo 3D-Secure 2.1 protocol (support biometric authentication), 2.2 (app-to-app flow), and 2.3 (SPC/ FIDO, device binding), which continuously improve the customer experience by adding more devices and more integration to the authentication flow.

### 3. Increase the exemption rate, but not at the expense of fraud

The rate of friction can directly impact the success rate. [A report by Ravelin](#) illustrates that the higher the percentage of frictionless payments is, the higher the authentication success rate. For example, the success rate in North America is 99% for 89% frictionless, compared to 55% in Europe, with 46% frictionless.

However, a high frictionless rate can still impact fraud rates. It is important to put in place rules that allow for the application of exemption requests while relying on scoring to assess the risk, and taking into account artificial intelligence. Data collection will become increasingly essential in the authentication process, as it feeds artificial intelligence, not only to feed Risk-Based Authentication (RBA) scoring, but also to enable the detection and prevention of phishing, adaptive authentication with risk scoring, and behavioural analysis.

## How Worldline assures a high level of security while improving the customer journey?

Worldline supports its customers throughout the 3D-Secure authentication chain:

- **Worldline Access Control Server** allows fraud prevention for e/m-commerce implementing 3D-Secure and strong authentication. It provides a rich back-office and artificial intelligence tool based on an analysis of past transactions to improve fraud management.
- **Worldline Trusted Authentication** protects your online services from unauthorised access with Strong Customer Authentication solutions for all devices, enabling password-less authentication thanks to transparent factors, biometrics, and FIDO authentication.
- **Worldline Digital Security Suite** protects your fleet with local and remote protection of your devices. It enables adaptive authentication methods and enrolment with our device eligibility scoring, thanks to our artificial intelligence model on device scoring and behavioural biometrics.

## With all these measures, where is the risk of fraud now?

The new authentication methods are reliable and have very low fraud rates. The main concern remains on the enrolment process which proves to be the weakest point of the chain. To enrol an authentication method, PSD2 requires to have two authentication factors. But, at this stage, the information known by the bank is the mobile phone number and the password. These two elements are most often the target of phishing attacks. The risk is now positioned on the cardholder.

It is important to avoid methods (both enrolment and authentication) that can be 'phished' (notably SMS OTP and password). Hence, the future lies in biometric and behavioural authentication methods, which are not very susceptible to phishing, but also in the use of the EU Digital Identity Wallet, which will simplify and secure the enrolment process.

[Click here for the company profile](#)

**WORLDLINE** 

[worldline.com](https://worldline.com)

**Worldline** is the European leader in the payment and transactional services industry. With innovation at the core of its DNA and thanks to a presence in 30+ countries, Worldline is the payment partner of choice for merchants, banks, public transport operators, government agencies, and industrial companies, delivering cutting-edge digital services.

# Signifyd

We discussed with Okan Ozaltin, General Manager for Payment Solutions at Signifyd, about the future of PSPs and how they can prevent fraud to ensure maximum conversion for merchants.



**Okan Ozaltin** is GM of Payment Solutions at Signifyd. He is focused on creating solutions that can be leveraged across the Payments Ecosystem to deliver higher authorisation rates and lower friction for customers. Before joining Signifyd, he was Payment Acquiring product lead for Fiserv in EMEA.

Okan Ozaltin ■ GM of Payment Solutions ■ Signifyd

## As ecommerce continues to expand, what did the last 12 months bring new to global merchants and PSPs?

Merchants and PSPs are now, more than ever, focusing on the shopping experience of customers and are trying to maximise their conversion. Fraud prevention tools continue to be a key topic that impacts merchants' overall conversion and revenue, as well as the overall customer shopping experience at the site. Very strict fraud solutions can cause friction or even prevent transactions from going through, which is an inconvenience to customers. Therefore, merchants need to set the right balance to maximise their revenues while looking after the end consumer. In EMEA, the PSD2/SCA regulation is well underway. SCA is working for some types of transactional fraud but not addressing all the emerging new fraud types such as ATO (Account Takeover), Friendly Fraud, and Return Abuse. In the past 12 months, we have also seen customers returning to brick-and-mortar stores, as countries are emerging out of COVID-19. Even so, ecommerce is still expected to grow meaningfully in the next few years. Most of the large merchants are focusing on their omnichannel strategies as they try to create seamless experiences for their customers, whether they shop in physical stores or online.

“ When merchants and PSPs think of fraud, they must consider the entire shopping experience, from account creation to the actual transaction, shipping, the fulfillment, and the return process.

## With customers demanding faster/real-time payments, how can merchants stop fraud that can also happen in 'real-time'? What are the main types of fraud they are experiencing?

Fraud occurs throughout different stages of the shopping experience; it doesn't just happen at the checkout or during the transaction. In the past, most fraud attempts focused on the checkout or transaction point, but we are now experiencing a shift in the modus operandi, so that it can be present during all stages, from account creation (Account Takeover) to after the item is shipped (chargeback fraud), and right through to the return process (returns fraud).

## Operating on a global level means complying with different regulations across different jurisdictions. How can merchants mitigate this complex process?

Every region has unique regulations, fraud tendencies, and market behaviours that impact a merchant's customer experience and its ability to maximise conversion or revenue. For example, in the EMEA, the PSD2 regulation enforces strong customer authentication (SCA) while maintaining the maximum rate of frictionless transaction. However, in the US, 3DS is used far less than in Europe and other regions, as it creates additional friction and problems. At the same time, LATAM has some of the lowest average overall authorisation rates in the world due to higher fraud rates and low issuer approval rates, which means it is imperative to work closely with experienced partners in the region that can both reduce fraud and provide a chargeback guarantee to the merchant. In other words, PSPs must use experienced providers that understand the nuances and differences in each region and offer appropriate service for merchants. →



Commonly, Signifyd works with large merchants that require different solutions in each of the regions they are operating in, which means there are no one-solution-fits-all scenarios. We provide different solutions for our merchants operating across these geographies as what works for customers in India might not be suitable for those in the US, and solutions for the EU market might not be relevant for Singapore, for example.

### What are the most useful tools global merchants and PSPs can opt for to detect fraud in time and successfully combat it? Can machine learning and AI positively impact anti-fraud solutions?

A single PSP or a merchant's historical data is not as diverse as a fraud provider's network of data that spans across merchants and PSPs. A good solution provider with access to large merchant side networks or consortium data would overlay machine learning and AI on top of that network, to maximise approvals and minimise false declines (declining good customers). Additionally, merchants and PSPs who leverage consortium data and use solutions that have machine learning and AI can provide a higher quality decision pre-authorization and achieve higher overall conversion rates. This leads to a higher level of customer satisfaction because the customer experiences less friction in the shopping process. A high-quality decision from the start reduces future fraud and chargeback problems that merchants and PSPs must deal with. Moreover, a chargeback guarantee solution based on AI and ML removes chargeback issues for merchants. Even with these solutions in place, fraud is never 100% preventable. So, if it does happen, merchants and PSPs should use AI and machine learning-based dispute tools to fight chargebacks and abuse. They can help identify challenging cases like friendly fraud and help prioritise the chargeback cases to fight, so that merchants get the best value for their effort.

### What are some of the ways that PSPs can be successful by differentiating themselves to win the market?

PSPs can differentiate themselves by offering value-added services such as fraud solutions, chargeback recovery, and guarantee. Utilising

a provider with advanced decisioning techniques, including machine learning and AI, will reduce fraud significantly, while increasing conversion rates. The key to ensuring that PSPs can differentiate themselves is to properly review, verify, and approve transactions by using data. The retail sector has become a plethora of data, much of which PSPs cannot access or view. By enabling PSPs to convert purchases based on the data available, behavioural trends, and assessment of overall risk, fraud protection providers like Signifyd can build trust across the payments landscape by powering Fearless Payments technology, one transaction at a time. Merchants cannot afford to lose money because they are not using effective anti-fraud tools to get the maximum conversion. If PSPs are offering these services to merchants, they can remain relevant even through tough economic times and still help merchants obtain maximum profits.

### Finally, how can Signifyd's core solutions contribute to protecting the shopper journey end-to-end, from fighting fraud to account protection, and compliance for a seamless SCA process?

Signifyd's core solution covers customers from the account creation stage to the fulfillment stage of order handling, as well as returns and disputes. Signifyd has one of the largest merchant site data networks in the world and our machine learning and AI tools use this network to make accurate decisions through the entire life cycle of the ecommerce shopping journey. Additionally, we can apply specific solutions in each region to maximise merchants' potential. For example, in the EMEA region, we provide transaction risk analysis and SCA exemption solutions, to maximise frictionless transactions for merchants, as part of the PSD2 regulation in Europe. In other regions where PSD2 regulations don't apply, like the US, Signifyd is able to boost approval rates for merchants while protecting against fraud and fraud losses. We are also closely working with issuers to provide them with additional data fields during the transaction process, which gives us, and our merchants, increased conversion rates, while reducing false declines.

[Click here for the company profile](#)



[signifyd.com](https://www.signifyd.com)

**Signifyd** provides an end-to-end Commerce Protection Platform that leverages its Commerce Network to maximise conversion, automate customer experience, and eliminate fraud and consumer abuse for retailers. Signifyd is headquartered in San Jose, CA., with locations in Denver, New York, Mexico City, Sao Paulo, Belfast, and London.



**Galit Shani-Michel** is VP of Payments at Forter. With over 15 years of experience, Galit has worked in various leadership roles, and is an expert in Online Payments, Fraud, Compliance, AML, GDPR, and fintech regulations.

Galit Shani-Michel ■ VP of Payments ■ Forter

In March 2022, the UK implemented the final piece of the second Payment Services Directive (PSD2), requiring customer-initiated payment transactions to be subjected to strong customer authentication (SCA), via a new method, such as two-factor authentication (2FA). PSD2 is designed to protect customers in the digital payment ecosystem from fraud, in particular Card Not Present (CNP) fraud, which has historically constituted the lion's share of card-related theft – amounting to an estimated EUR 1.5 billion in 2019.

However, it also introduces extra friction into the payment process. This can result in lost revenue, as customers fail to complete transactions for a variety of reasons.

Additionally, not all fraud is prevented by SCA, as fraudsters continuously develop new ways to circumvent 2FA. Thus, there is a balance to be struck between protecting customers and safeguarding revenue.

Now, nine months after full implementation, we have sufficient data from the UK and other major retail markets in Europe to learn what impact PSD2 is having on ecommerce fraud and revenues. The picture is mixed, to say the least, with key findings showing that:

### Lost revenues are significant

Forter's analysis shows that, across the UK, Germany, France, Spain, and Italy merchants are missing out on up to 8-10% of revenue, as a result of SCA application using 3D-Secure (3DS).

In the UK, in cases where SCA has been applied using 3DS to transactions of any amount, only 79% of transactions are completed. Eight percent are abandoned by the customer, 11% fail due to the

customer entering incorrect details, and 2% experience a technical issue that prevents the transaction success. This means that merchants are losing more than 20% of transactions every time 3DS is applied. Considering that in the UK 3DS is applied to 10% of transactions, on average, this can seriously impact the revenue.

### Mobile 3DS failure rates exceed web-based failures

Mobile commerce is rapidly catching up with its desktop counterpart. 15% percent **of total retail sales were conducted through a mobile phone in 2021** – but challenges remain. Consumers don't like typing on tiny screens and having to enter data multiple times adds unwelcome friction. Merchants and PSPs are working hard to overcome this by storing key information such as logins, delivery addresses, and payment data to autofill forms, wherever possible.

However, these efforts can become challenging and frustrating when it comes to the application of 3DS, and that's reflected in our findings: while 81% of transactions subjected to 3DS via the web were successful, that figure drops to 72% on mobiles. This disparity existed across all regions to different extents, with almost a 13% drop in 3DS success between web and mobile in Germany.

Clearly, merchants and 3DS providers must collaborate to optimise the customer experience on mobiles, so merchants can successfully make the transition from ecommerce to m-commerce and avoid leaving revenue on the table. Implementing effective Transaction Risk Analysis (TRA) and working with multiple PSPs so exemptions can be requested wherever possible is a key route to reducing friction, and one that should be a priority for businesses to reduce lost revenue. →

## The UK has adapted best to PSD2

Among the five biggest European retail markets, the UK has the highest authorisation rate (92%) and completion rate (90%) for 3DS transactions. This compares to an average across the markets of 88% authorisation rate and just an 82% completion rate. It seems that, despite being the last region to fully implement PSD2 – or perhaps because of this – the UK payments ecosystem has adapted best.

## The UK challenger banks are leading the SCA charge

Looking at the data in detail reveals that UK challenger banks have the highest 3DS success rate, with 87% of all transactions completed successfully. The focus on user experience and seamless service underpinning the challenger bank ethos may explain their success in guiding customers through 3DS challenges.

## What's the safe and compliant way to optimise revenue?

Given SCA has such a significant impact on transactions, must merchants use it 100% of the time? The simple answer is no; merchants can use TRA exemptions to legally bypass the SCA requirement. This boost to transaction volumes can increase revenue but will also increase the risk of fraud and chargebacks, so it's important for merchants to use a fraud prevention tool to decide when exemptions should be used.

## PSD2: anti-fraud tool, conversion killer, or both?

PSD2's SCA requirement undoubtedly adds security to CNP payments, but it also adds friction leading to the loss of legitimate transactions. The above data shows that PSD2 has certainly had a negative effect on conversions, leading to lost revenue and customer frustration at a time when, more than ever, merchants need to strengthen customer relationships and maximise every transaction opportunity.

In terms of fraud, PSD2 may have hardened one fraud vector, but this has only shifted the problem. Forter's research across Europe has detected a considerable increase in alternative payment method fraud (such as gift cards), which rose 60% in 2021 compared to the pre-PSD2-enforcement period in 2020. We also found a 30% increase in fraud pressure around Item Not Received (INR) tactics. Fraudsters are going elsewhere, and this underlines the need for multi-channel fraud protection, as PSD2 is not a silver bullet.

Nevertheless, consumers are better protected overall, so it is now incumbent on merchants and PSPs to develop smarter ways to provide a seamless customer experience while blocking fraud. And, as challenger banks lead the charge, their legacy counterparts should take a leaf from their ledger to raise the level of user experience and limit the impact of PSD2 on merchant revenues.



[forter.com](https://forter.com)

**Forter** is the Trust Platform for digital commerce. We make accurate, instant assessments of trustworthiness across every step of the buying journey. Forter helps businesses prevent fraud, maximise revenue, and deliver superior experiences for consumers. This is why it has been trusted to process more than USD 500 billion in transactions.

# Who Is Who in Fraud Prevention













This chapter is dedicated to notable key players in the industry who are constantly chasing and deterring fraud by eliminating pain points, while adapting to customers' evolving expectations. This year's edition of our report brings an overview of key players' core services in fraud prevention.








# Overview of Key Players' Core Services in Fraud Prevention

Fraud/Risk Management and Decisioning Platform			
1975	1996	2002	2008
 ACI Worldwide <small>Real-Time Payments</small>	 netcetera	 PingIdentity.	 Accertify <small>AN AMERICAN EXPRESS COMPANY</small>  entersekt <small>and you're in.</small>
2011		2012	2016
 sift	 Signifyd	 checkout.com	 Nethone
2019		2021	
 caf.	 FUGU <small>EVERY PAYMENT COUNTS</small>	 kipp	 Darwinium








Year founded

Consumer Authentication			
1973	1996	2002	2008
 WORLDLINE	 netcetera	 PingIdentity.	 Accertify <small>AN AMERICAN EXPRESS COMPANY</small>  entersekt <small>and you're in.</small>
2011		2016	2019
 sift	 Signifyd	 Nethone	 caf.  FUGU <small>EVERY PAYMENT COUNTS</small>

Year founded

Identity Verification				
1996	2002	2008	2011	2016
 netcetera	 PingIdentity.	 entersekt <small>and you're in.</small>	 Signifyd	 Nethone
2019				
 caf.		 FUGU <small>EVERY PAYMENT COUNTS</small>		

Year founded

Behavioural Biometrics		
1973	1996	2008
 WORLDLINE	 netcetera	 Accertify <small>AN AMERICAN EXPRESS COMPANY</small>  entersekt <small>and you're in.</small>
2011		2019
 Signifyd		 Nethone  caf.








Year founded

Researched by © The Paypers, 2022

# Overview of Key Players' Core Services in Fraud Prevention

Data Provider and Intelligence				
1996	2002	2008	2011	2021
				




Year founded

Chargebacks Management				
2008	2011			2012
				
2016		2019		
				


Year founded

Bot Risk Management	
2011	2016
	
	

Year founded

KYB / Merchant Onboarding	
2011	2019
	
	

Year founded

KYC		
2011	2016	2019
		
		


Year founded

Researched by © The Paypers, 2022

# Company Profiles



Solution providers present their approach against the increasing fraud challenges and uncover the potential of their latest technologies, their reach in the industry, and their successful business model for the specific target group they serve.

Company		Accertify	
		<p>Accertify is a leading provider of fraud prevention, chargeback management, digital identity, and payment gateway solutions to customers spanning ecommerce, financial services, and other diverse industries worldwide. Accertify's layered risk platform, machine learning backbone, and rich reputational community database enables businesses to address challenges across the entire customer journey without impacting the customer experience.</p>	
Background information			
Year founded	2008		
Website	<a href="https://accertify.com">accertify.com</a>		
Target group	Merchants/ecommerce PSP/acquirers Bank/FS		
Supported regions	Global		
Contact	Michelle DiDomenico – <a href="mailto:mdidomenico@accertify.com">mdidomenico@accertify.com</a>		
Company's tagline	We've Got Your Back		
Member of industry association and/or initiatives	MRC, FIDO, SOTER, Payments Ed, NRF, Amadeus		
Core solution			
Core solution/problems the company solves	Fraud/risk management and decisioning platform Customer authentication Behavioural biometrics Chargebacks management Data provider and intelligence Enable organisations to mitigate risk/fraud, increase revenues, and deliver a differentiated customer experience.		
Technology			
	Cloud enabled		
Data input			
Identity verification	proprietary capability	third party	both
Personally Identifiable Information (PII) validation			x
Email verification			x
Phone verification		x	
Social verification		x	
Compliance check		x	
Online authentication	proprietary capability	third party	both
Behavioural biometrics	x		
Device fingerprinting	x		
Geo-location	x		
Remote access detection	x		
Mobile app push	x		
3-D Secure 2.0		x	
One-time passwords		x	
Knowledge-based authentication		x	



Intelligence	proprietary capability	third party	both
Abuse list	x		
Monitoring	x		
Address verification		x	
Credit bureau		x	
Information sharing	x		
<b>Data ingestion/third-party data</b>			
Stateless data ingestion and augmentation		x	
<b>Methodology</b>			
Machine learning	Hybrid		
<b>Decisioning</b>			
	Manual review Case management Decision orchestration		
<b>Chargeback management</b>			
	Chargeback dispute Guaranteed fraud protection		
<b>Business model</b>			
Fraud prevention partners	American Express, Mastercard, Visa, Lexis Nexis, Credit Bureaus, Amadeus		
Number of employees	500		
Future developments	C.A.R.E (Claims, Adjustments, Returns, Exchanges) will be a future development for Accertify. By tracking customer interactions and aggregating data around key metrics and abuse indicators, C.A.R.E expands a merchant's capacity to stop financial loss via informed, data-driven decisions. We will also continue to enhance our industry-specific machine learning models. More information on this and other enhancements is available upon request.		
<b>Customers</b>			
Customers reference	Please reference our case studies and customers listed on our website.		
	View company profile in online database*		
	*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a> .		




## Solutions for the Entire Customer Journey

Accertify, Inc., a wholly-owned subsidiary of American Express, is a leading provider of fraud prevention, digital identity, device intelligence, chargeback management, and payment gateway solutions to customers spanning diverse industries worldwide. Accertify's suite of products and services help companies grow their business by driving down the total cost of fraud, simplifying business processes, and ultimately increasing revenue.



For more information, please visit [www.accertify.com](http://www.accertify.com)

Company		ACI Worldwide	
		<p>ACI Worldwide delivers the software and solutions that power the global economy. Our mission-critical real-time payment solutions enable corporations to process and manage digital payments, power omni-commerce payments, present and process bill payments, and manage fraud and risk.</p>	
Background information			
Year founded	1975		
Website	<a href="https://www.aciworldwide.com/">https://www.aciworldwide.com/</a>		
Target group	<p>Merchants: retail, gaming and digital goods, travel, telecommunications, grocery, restaurants, fuel and convenience, hospitality.</p> <p>Merchant intermediaries/payment intermediaries, banking, consumer finance, insurance, government, higher education, healthcare.</p> <p>Marketplaces</p> <p>PSP</p> <p>Fintech</p> <p>Banks</p> <p>Brokers, crypto exchange, FX brokers</p>		
Supported regions	Global		
Contact	Annett Van de Bunt, Head of Marketing Payments Solutions		
Company's tagline	Driving the digital transformation of banks, merchants, and billers to help them meet the real-time payment needs of their consumers and business customers.		
Member of industry association and/or initiatives	Merchant Risk Council (MRC), NRF, MAG, Vendorcom, EBA, US Faster Payments Council, Open Banking, ATMIA, CEPS/ECRI, InfraGard, IFX, NACHA, NSPO, PSR, SWIFT, US Payments Forum, Women in Payments.		
Core solution			
Core solution/problems the company solves	<p>ACI Worldwide serves the full payment ecosystem, processing and managing digital payments, managing fraud and risk for merchants, banks, and intermediaries.</p> <p>The company enables omni-commerce payments through its payments and fraud orchestration platform. ACI Fraud Management is a real-time, cloud-based, managed service that uses advanced AI (Artificial Intelligence), ML (Machine Learning) and behavioural analytics to identify and assess inconsistent and unexpected patterns and behaviours. The solution automatically advises and alerts enterprises and merchants about potential threats or anomalies.</p>		
Technology			
	Cloud-enabled		
Data input			
Identity verification	proprietary capability	third party	both
Identity document scanning		x	
Personally Identifiable Information (PII) validation		x	
Small transaction verification	x		
Email verification			x
Phone verification			x
Social verification		x	
Credit check		x	
Compliance check		x	
Online authentication	proprietary capability	third party	both
Behavioural biometrics		x	
Physical biometrics		x	

Device fingerprinting		x	
Geo-location		x	
Mobile app push	x		
3-D Secure 2.0	x		
Hardware token	x		
One-time passwords	x		
Knowledge-based authentication		x	
<b>Intelligence</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Abuse list			x
Monitoring	x		
Address verification		x	
Credit bureau		x	
<b>Data ingestion/third-party data</b>			
Stateless data ingestion and augmentation		x	
<b>Methodology</b>			
Machine learning	ACI patented AI Incremental learning providing Self-Learning ML models. ACI's incremental learning algorithm allows machine learning models to adjust to new behaviours without the need to re-learn everything they already know. This means that new data can be input on a daily basis and new behaviours can be identified in near real-time. Machine learning model performance lasts for longer without degradation and reduces the need for often costly model refreshes. It improves fraud detection by up to 85% and can also reduce fraud losses by up to 75%. In production, ACI incremental learning has been shown to outperform traditional ML by 15%.		
<b>Decisioning</b>			
	Manual review Case management Decision orchestration		
<b>Chargeback management</b>			
	Chargeback Representment Chargeback Indemnification – for more information please visit <a href="https://www.aciworldwide.com/solutions/chargeback-protection">https://www.aciworldwide.com/solutions/chargeback-protection</a>		
<b>Business model</b>			
Pricing model	More information available upon request		
Fraud prevention partners	ACI Worldwide augments its Fraud Management solution with third-party partners like Riverty (Avarto), TransUnion, Ekata.		
Year over year growth rate	USD 1.4 billion FY2021 revenue +6% growth - USD 384 million FY2021 Adjusted EBITDA +7% - USD 128 million FY2021 Net Income +76%. For more information please visit <a href="https://investor.aciworldwide.com/investor-relations">https://investor.aciworldwide.com/investor-relations</a>		
Number of employees	4,000		
Future developments	More information available upon request		
<b>Customers</b>			
Customers reference	Customer information upon request - For all ACI Worldwide case studies please visit: <a href="https://www.aciworldwide.com/insights/case-studies">https://www.aciworldwide.com/insights/case-studies</a>		
	View company profile in online database*		
	*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a> .		

# Turning Advanced Fraud Prevention Into a Revenue Generator


ACI® Fraud Management™ is a real-time, cloud-based, managed service that uses advanced artificial intelligence, machine learning and behavioral analytics to identify and assess inconsistent and unexpected patterns and behaviors.

The solution automatically advises and alerts enterprises and merchants to potential threats or anomalies. It delivers enhanced security orchestration to achieve seamless shopping experiences in real time.

## Ready to get started?

Visit [aciworldwide.com/fraud](https://aciworldwide.com/fraud) to learn how the ACI Fraud Management solution helps guarantee higher acceptance rates and lower chargebacks.



Company		CAF	
		CAF is a leading provider of end-to-end identity verification, proofing, and authentication solutions that combine advanced computer vision ML models, an AI-powered decisions engine, and sophisticated identity orchestration with an extensive collection of biometrics and identity databases.	
<b>Background information</b>			
Year founded	2019		
Website	<a href="https://caf.io/">https://caf.io/</a>		
Target group	Merchants/ecommerce PSP/acquirers SMB Banks/FS Corporate Fintech Telecom		
Supported regions	US, Europe, LATAM		
Contact	<a href="mailto:comercial@caf.io">comercial@caf.io</a> , <a href="mailto:pr@caf.io">pr@caf.io</a> , <a href="mailto:marketing@caf.io">marketing@caf.io</a>		
Company's tagline	Experts in Identity		
Member of industry association and/or initiatives	MRC		
<b>Core solution</b>			
	Fraud/risk management and decisioning platform Customer authentication Identity verification Behavioural biometrics KYB/Merchant onboarding KYC		
Core solution/problems the company solves	CAF combines an AI-powered decision engine and sophisticated identity orchestration with an extensive collection of biometrics and identity databases to deliver a better balance between security and user experience		
<b>Technology</b>			
	Cloud native		
<b>Data input</b>			
<b>Identity verification</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Identity document scanning	x		
Video scanning	x		
Personally Identifiable Information (PII) validation	x		
Email verification			x
Phone verification			x
Social verification		x	
Compliance check			x
<b>Online authentication</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Behavioural biometrics			x
Device fingerprinting			x
Geo-location			x
Remote access detection			x


Intelligence	proprietary capability	third party	both
Abuse list	x		
Monitoring	x		
Address verification			x
Credit bureau		x	
Information sharing			x
<b>Methodology</b>			
Machine learning	Supervised ML		
<b>Decisioning</b>			
	Manual review Case management Decision orchestration		
<b>Business model</b>			
Pricing model	Pricing is per transaction and based on volume and complexity		
Number of employees	280		
<b>Customers</b>			
Customers reference	Magalu, Vivo, Localiza.		
	View company profile in online database*		
	*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a> .		

# Who is real on digital?

More digital interactions mean more risks.  
Caf knows who is real in the digital world.





Company		Chargebacks911		
		<p>Founded in 2011, Chargebacks911 is the first global company fully dedicated to mitigating chargebacks and eliminating chargeback fraud. As an industry-leading innovator, Chargebacks911 is credited with developing the most effective strategies for helping businesses manage disputes and reduce loss in various industries and sectors within the payments space.</p>		
Background information				
Year founded	2011			
Website	<a href="https://chargebacks911.com">chargebacks911.com</a>			
Target group	Merchants/ecommerce			
Supported regions	Global			
Contact	Jarrod Wright, VP Marketing			
Company's tagline	Challenge the Status Quo			
Core solution				
Core solution/problems the company solves	<p>Chargebacks management</p> <p>The innovative suite of proprietary technologies optimise profitability through the most comprehensive chargeback management. Identifies true chargeback sources and deploys the most effective solution for increased revenue recovery.</p> <p>Performance-based ROI guarantee.</p>			
Technology				
	Hybrid			
Data input				
Online authentication	proprietary capability	third party	both	
Behavioural biometrics	More information available upon request			
Physical biometrics	More information available upon request			
Device fingerprinting	More information available upon request			
Geo-location	More information available upon request			
Remote access detection	More information available upon request			
Mobile app push	More information available upon request			
3-D Secure 2.0	More information available upon request			
Knowledge-based authentication	More information available upon request			
Intelligence	proprietary capability	third party	both	
Abuse list	More information available upon request			
Monitoring	More information available upon request			
Address verification	More information available upon request			
Information sharing	More information available upon request			
Data ingestion/third-party data				
Stateless data ingestion and augmentation	More information available upon request			
Methodology				
Machine learning	Hybrid			
Decisioning				
	Case Management			

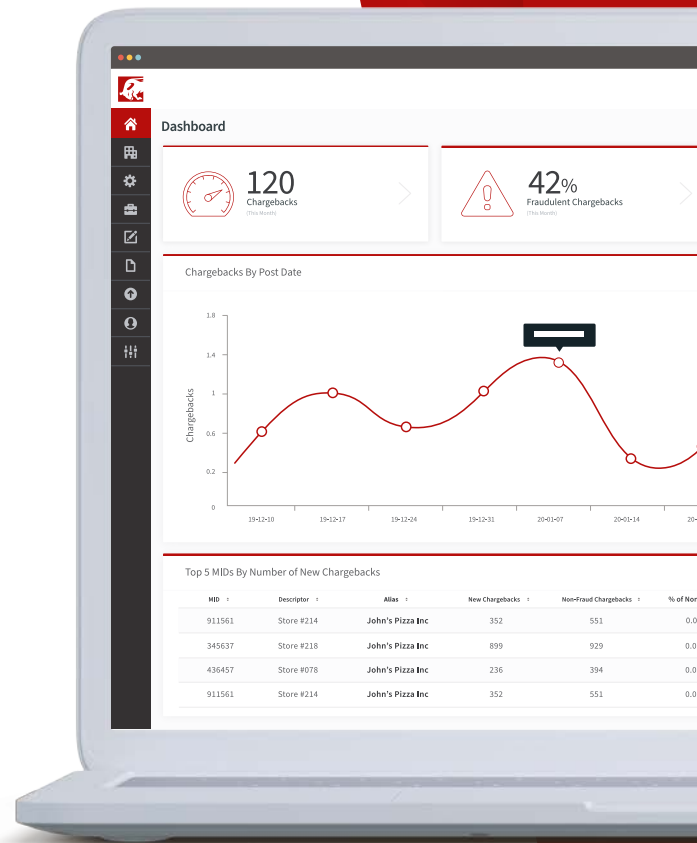
<b>Chargeback management</b>	
	Chargeback dispute Guaranteed fraud protection
<b>Business model</b>	
Pricing model	Tiered payment levels of service/pricing, from consultation to full-service
Fraud prevention partners	Ethoca Alerts, Verifi Alerts
Year over year growth rate	15%
Number of employees	Approximately 600
Future developments	Chargeback indemnification
<b>Customers</b>	
Customers reference	Gap, Nutrisystem, Harley-Davidson, Hello Fresh
	<a href="#">View company profile in online database*</a>
	*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a> .



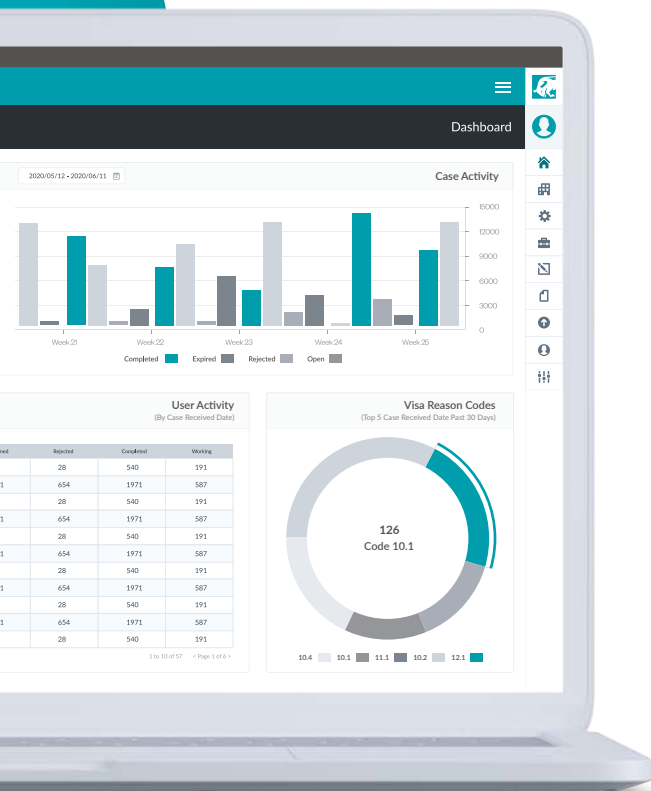
# The leading dispute resolution and chargeback management technology for *merchants*

Better data and advanced technology transform chargebacks from a liability to an asset. 250 plug-in connections allow merchants to be onboarded faster and without development resources.

[chargebacks911.com](https://chargebacks911.com)




## the only **End to End** solution engagement from transaction to dispute resolution




# Automated dispute processing and turnkey SAAS products for *financial institutions*

With our suite of back-office solutions, financial institutions can automate dispute management, improve data security, maintain compliance, and better serve the needs of their merchants.

[fi911.com](https://fi911.com)

Company		Darwinium	
 <b>Darwinium</b>		Darwinium is the world's first Customer Protection Platform, operating across every digital interaction: web, apps, and APIs. Darwinium proprietary similarity signatures and risk-based orchestration operates at the perimeter edge, continuously assessing every digital interaction to identify bad behaviour, streamline risk decisions, and automate remediation in real time.	
Background information			
Year founded	2021		
Website	<a href="https://www.darwinium.com/">https://www.darwinium.com/</a>		
Target group	Merchants/ecommerce Banks/FS Fintech SMBs and Enterprise		
Supported regions	Global		
Contact	Rebekah Moody		
Company's tagline	Continuous Customer Protection Across Your Digital Perimeter		
Member of industry association and/or initiatives	MRC, Gartner		
Core solution			
Core solution/problems the company solves	Fraud/risk management and decisioning platform Simplify and automate fraud & security operations. Understand trust/risk across complete user journeys. Make faster, better decisions closer to customer data. Dynamically tailor digital journeys to improve user experience.		
Technology			
	Native Cloud On-premise		
Data input			
Identity verification	proprietary capability	third party	both
Identity document scanning		x	
Personally Identifiable Information (PII) validation			x
Small transaction verification		x	
Email verification		x	
Phone verification		x	
Social verification		x	
Credit check		x	
Compliance check		x	
Online authentication	proprietary capability	third party	both
Behavioural biometrics	x		
Physical biometrics		x	
Device fingerprinting	x		
Geo-location	x		
Remote access detection	x		
Mobile app push		x	
3-D Secure 2.0			x
Hardware token		x	
One-time passwords		x	
Knowledge-based authentication			x

Intelligence	proprietary capability	third party	both
Abuse list			x
Monitoring	x		
Address verification		x	
Credit bureau		x	
Information sharing		x	
<b>Data ingestion/third-party data</b>			
Stateless data ingestion and augmentation		x	
<b>Methodology</b>			
Machine learning	Rule-based Supervised ML Unsupervised ML Darwinium supports PMML industry standard for third-party models.		
<b>Decisioning</b>			
	<b>Decision Orchestration:</b> This includes low code, no-code, and all-the-code options. Self-supervised ML. Proprietary real-time similarity signatures. Rules engine and custom ML model execution. Champion/Challenger. Simulation.		
<b>Business model</b>			
Pricing model	Pricing is per transaction based on volume, with economies of scale		
Fraud prevention partners	Integrate any third-party API		
Year over year growth rate	Not disclosed		
Number of employees	17		
Future developments	Security and Fraud Marketplace Web Worker support across further CDNs Advancements in ML at the Edge API Discovery Simulation		
<b>Customers</b>			
Customers reference	Not disclosed		
	View company profile in online database*		
	*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a> .		

Company		Entersekt	
		<p>Entersekt ensures that digital financial transactions are frictionless and secure. The company provides a single cross-channel platform for financial services institutions to meet authentication requirements and optimise user experiences. With a range of options available for deployment and configuration, Entersekt's solutions are fully customisable across all channels and devices.</p>	
Background information			
Year founded	2008		
Website	<a href="http://www.entersekt.com">www.entersekt.com</a>		
Target group	Ecommerce Banks Fintech Telecom		
Supported regions	The US, Europe, Middle East, Africa, LATAM		
Contact	<a href="mailto:info@entersekt.com">info@entersekt.com</a>		
Company's tagline	And you're in!		
Member of industry association and/or initiatives	FIDO; W3C; EMVCo; WASPA; MobeyForum; Mobile Connect; Bank ID; The Payments Association		
Core solution			
Core solution/problems the company solves	<p>Fraud/risk management and decisioning platform Customer authentication Identity verification Behavioural biometrics</p> <p>Entersekt's strong device identity and authentication solution helps secure digital transactions across channels and ensures compliance with the latest regulations and frameworks.</p>		
Technology			
	On-premise Native cloud Hybrid		
Data input			
Identity verification	proprietary capability	third party	both
Identity document scanning		x	
Video scanning		x	
Phone verification			x
Online authentication	proprietary capability	third party	both
Behavioural biometrics			x
Physical biometrics			x
Device fingerprinting	x		
Geo-location	x		
Mobile app push	x		
3-D Secure 2.0	x		
Hardware token			x
One-time passwords	x		
Knowledge-based authentication	x		
Intelligence	proprietary capability	third party	both
Abuse list	x		

Data ingestion/third-party data	
Stateless data ingestion and augmentation	x
Methodology	
Machine learning	Rule-based Supervised ML Unsupervised ML Hybrid
Decisioning	
	Decision orchestration
Business model	
Pricing model	Please contact <a href="mailto:info@entersekt.com">info@entersekt.com</a> for more information on pricing across deployment options.
Fraud prevention partners	NuData Security; Featurespace
Year over year growth rate	Please contact <a href="mailto:info@entersekt.com">info@entersekt.com</a> for more information.
Number of employees	150+
Future developments	Open Banking; digital identity
Customers	
Customers reference	Absa; African Bank; Bayern Card Services; Capitec Bank; Coutts; Discovery; Ecobank; FirstBank of Colorado; Hanseatic Bank; Investec; Nedbank; Old Mutual; Pluscard; Swisscard. For others not in the public domain, please contact us at <a href="mailto:info@entersekt.com">info@entersekt.com</a> .
	View company profile in online database*
	*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a> .

e-Commerce fraud is out.  
**Great UX and transaction success are in.**



Global projections show that e-commerce trade will top **€6 trillion by 2024**. Unfortunately, fraud will rise just as rapidly.

Don't be caught out by weak or complicated online payment security. Take back control with Entersekt's **market-leading 3D Secure** solution.



**Eliminate fraud.**

Beat cybercriminals with advanced, pre-integrated e-commerce transaction protection, including risk intelligence.



**Boost transactions.**

Enjoy transaction success rates that are 22% higher than the market average, thanks to a more comprehensive solution.



**Enhance user experience.**

Enable your customers to transact seamlessly, without the hassle of OTPs. No more authentication complication!


**Talk to an expert today to learn about these and other unique features:**

- Full control of your ACS
- 22 Configurable user journeys
- Step-up and fallback mechanisms beyond traditional OTPs
- Access to transactional data
- Continuous 3D Secure & PSD2 compliance


**Scan the code or email [info@entersekt.com](mailto:info@entersekt.com).**





Company		FUGU	
		<p>FUGU offers a new breed of payment anti-fraud solution, monitoring payments post-checkout, helping merchants safely accept transactions they currently lose to fraud, false declines, payment churn.</p> <p>FUGU is the first multi-tier fraud prevention solution fighting fraud at various points along the transaction life cycle, covering a wide variety of risk patterns (Friendly Fraud) and new innovative payment models.</p>	
Background information			
Year founded	2019		
Website	<a href="https://fugu-it.com">https://fugu-it.com</a>		
Target group	Merchants/ecommerce PSP/acquirers SMBs Banks/FS		
Supported regions	Global		
Contact	<a href="mailto:Sales@fugu-it.com">Sales@fugu-it.com</a>		
Company's tagline	Every Payment Counts		
Member of industry association and/or initiatives	More information available upon request.		
Core solution			
Core solution/problems the company solves	Fraud/ risk management and decisioning platform Customer authentication Identity verification Chargebacks management KYB/Merchant onboarding KYC  FUGU provides a one-stop-shop payment risk platform that reduces false declines based on continuous risk analysis far after order creation, suspicious customer verifications, and automatic chargeback representations.		
Technology			
	Native cloud		
Data input			
Identity verification	proprietary capability	third party	both
Identity document scanning	x		
Small transaction verification	x		
Email verification			x
Phone verification			x
Social verification	x		
Compliance check		x	
Online authentication	proprietary capability	third party	both
Physical biometrics	x		
Device fingerprinting			x
Geo-location			x
3-D Secure 2.0			x
One-time passwords			x

Intelligence	proprietary capability	third party	both
Abuse list	x		
Monitoring	x		
Address verification			x
<b>Data ingestion/third-party data</b>			
Stateless data ingestion and augmentation		x	
<b>Methodology</b>			
Machine learning	Hybrid		
<b>Decisioning</b>			
	Manual review Case management		
<b>Chargeback management</b>			
	Chargeback dispute Guaranteed fraud protection		
<b>Business model</b>			
Pricing model	Hybrid model of per transaction and based on volume and complexity OR SaaS-based pricing model based on customer-defined rules.		
Year over year growth rate	200%		
Number of employees	20		
Future developments	Video verification, Promise To Pay capability guaranteeing shipment for failed payments.		
<b>Customers</b>			
Customers reference	E420, XBO (Crypto), Payne, Adika, Borboun Central, Underoutfit		
	View company profile in online database*		
	*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a> .		

Company		Kipp	
		<p>Kipp is a global fintech company enabling issuing banks and merchants to jointly approve legitimate transactions that are currently being declined. The company's platform optimises the traditional payment model for increased revenue, customer satisfaction, and loyalty. Kipp's founders and team are fintech veterans and payment optimisation professionals.</p>	
<b>Background information</b>			
Year founded	2021		
Website	<a href="http://www.letskip.com">www.letskip.com</a>		
Target group	Merchants/ecommerce Banks/FS		
Supported regions	Europe, the UK, the US		
Contact	Mr. Chanan Lavi, CEO and Co-Founder		
Company's motto	Authorize More		
Member of industry association and/or initiatives	MRC		
<b>Core solution</b>			
Core solution/problems the company solves	<p>Risk management and decisioning platform Data provider and intelligence</p> <p>Kipp's technology leverages the aligned interests of issuers and merchants to authorise more legitimate transactions by providing an automated and seamless system that shares data and splits the risk costs in real-time, based on predefined rules.</p>		
<b>Technology</b>			
	Cloud enabled		
<b>Data input</b>			
<b>Intelligence</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Information sharing			x
<b>Data ingestion/third-party data</b>			
Stateless data ingestion and augmentation		x	
<b>Methodology</b>			
Machine learning	Rule-based		
<b>Business model</b>			
Pricing model	Percentage, transaction-based.		
Fraud prevention partners	Fraudio, Fraugster, nSure.ai		
Number of employees	15		
Future developments	More information available upon request.		
<b>Customers</b>			
Customers reference	More information available upon request.		
	View company profile in online database*		
	*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a> .		



# Its time to optimize your payments with Kipp

Merchants and Issuers can collaborate by sharing data and the cost of risk to approve more transactions.

**Keep your customers happy and your revenue growth!**



Increase revenue




Maintain customer satisfaction



Reduce operational costs



Ensure customer loyalty

Company		Netcetera	
		<p>As a market leader in payment security, we offer innovative digital payment solutions with a strong focus on convenience, security, and mobile use. Our customers rely on our high-quality, scheme-certified products for 3-D Secure, mobile contactless payment, digital wallets, risk-based and convenient authentication or digital banking apps for optimised banking.</p>	
Background information			
Year founded	1996		
Website	<a href="http://www.netcetera.com">www.netcetera.com</a>		
Target group	Merchants/ecommerce PSP/acquirers Banks/FS Corporate Fintech		
Supported regions	Global		
Contact	<a href="mailto:info@netcetera.com">info@netcetera.com</a>		
Company's tagline	Software matters		
Member of industry association and/or initiatives	EMVCo associate, EPSM, MC Digital Partner, and Visa Ready		
Core solution			
Core solution/problems the company solves	Fraud/risk management and decisioning platform Customer authentication Identity verification Behavioural biometrics Data provider and intelligence  3DS Service provides convenient, but yet secure authentication of ecommerce transactions. The service has high flexibility and configurability, ensuring fast and easy deployment of 3DS for the banks.		
Technology			
	Cloud based		
Data input			
Identity verification	proprietary capability	third party	both
Email verification	x		
Phone verification			x
Online authentication	proprietary capability	third party	both
Physical biometrics		x	
Device fingerprinting	x		
Geo-location		x	
Remote access detection		x	
Mobile app push			x
3-D Secure 2.0	x		
Hardware token	x		
One-time passwords	x		
Knowledge-based authentication	x		
Intelligence	proprietary capability	third party	both
Abuse list		x	
Monitoring			x

<b>Methodology</b>	
Machine learning	Rule-based Supervised ML
<b>Decisioning</b>	
	Case management
<b>Business model</b>	
Pricing model	Pricing is per transaction and based on volume and complexity
Fraud prevention partners	Inform
Year over year growth rate	46% transactions growth
Number of employees	800+
Future developments	multiple third-party partners, FIDO SPC support
<b>Customers</b>	
Customers reference	<a href="https://www.netcetera.com/home/company/track-record.html">https://www.netcetera.com/home/company/track-record.html</a>
	<b>View company profile in online database*</b>
	*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a> .



Online fraudsters are always on the prowl  
**But we're always one step ahead**

**26** years of experience  
providing 3DS solutions



The latest  
anti-fraud technology




Lightning-fast  
implementation



Impeccable customer  
service, 24/7

Get in touch today  
[www.netcetera.com](http://www.netcetera.com)



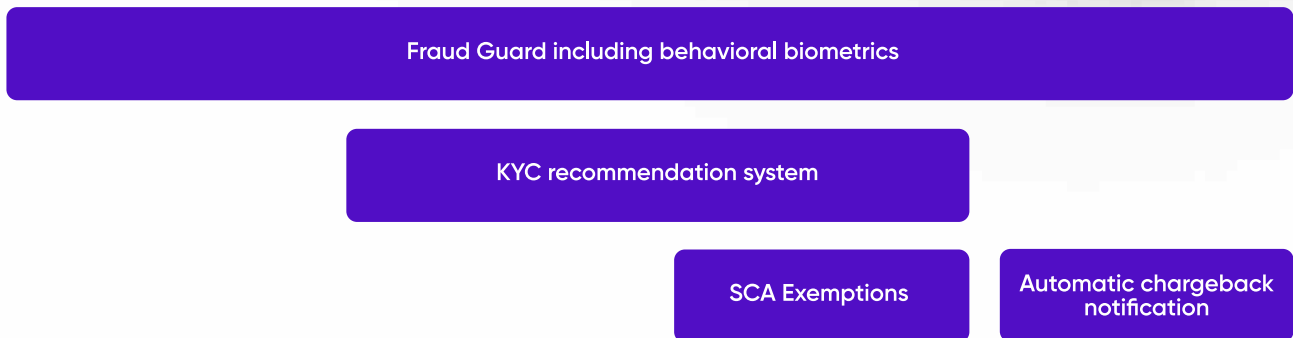
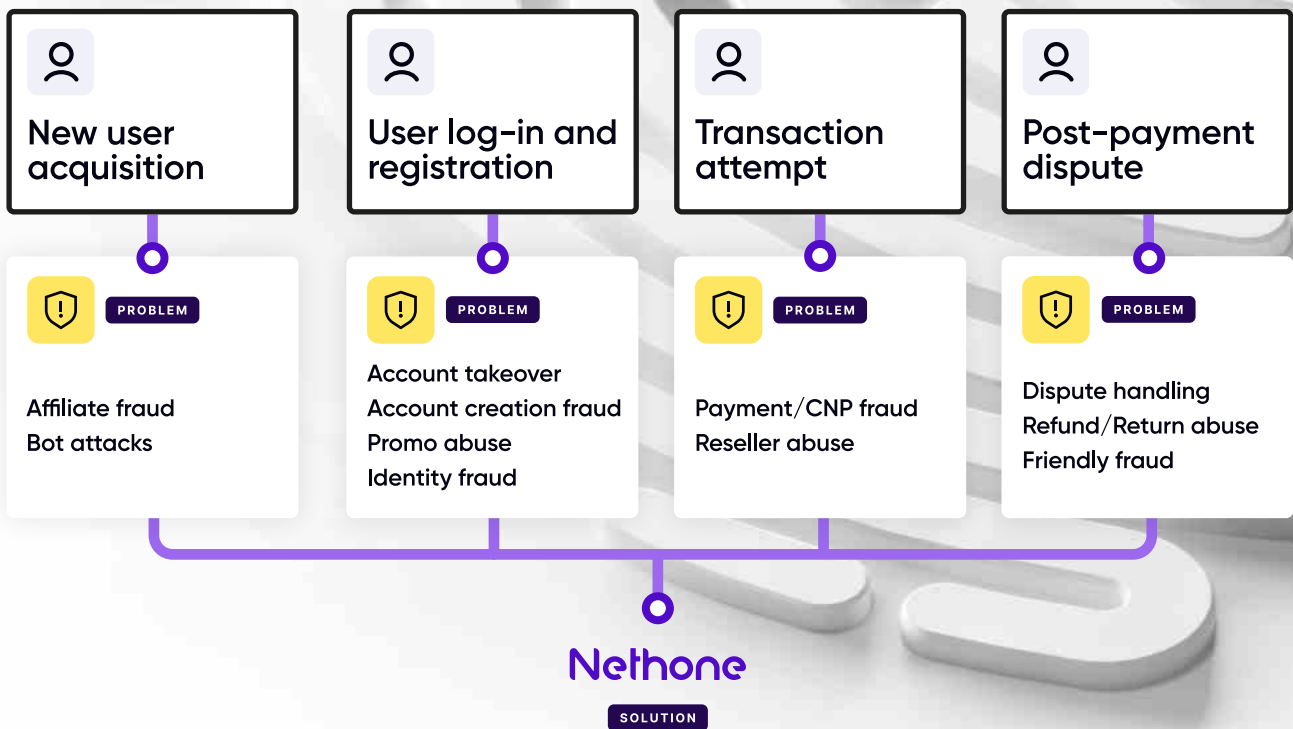
Company		Nethone	
		<p>Nethone is a machine learning-based fraud prevention SaaS company that enables ecommerce merchants and financial institutions to holistically understand their end-users — also referred to as Know Your Users (KYU). With our proprietary online user profiling and AI-powered tools, we can block all risky users without friction to the good ones by exhaustively screening every single one.</p>	
Background information			
Year founded	2016		
Website	<a href="https://nethone.com/">https://nethone.com/</a>		
Target group	Merchants/ecommerce Banks/FS PSP/acquirers Fintech		
Supported regions	Europe, Middle East, LATAM, US, APAC		
Contact	<a href="mailto:contact@nethone.com">contact@nethone.com</a>		
Company's tagline	Know Your Users™, reject only fraudsters		
Member of industry association and/or initiatives	Merchant Risk Council, Center for Financial Professionals. More information available upon request.		
Core solution			
Core solution/problems the company solves	<p>Real-time fraud, risk management, and decisioning platform</p> <p>Customer authentication</p> <p>Identity verification</p> <p>Behavioural biometrics</p> <p>Chargebacks management</p> <p>Bot prevention</p> <p>Risk-based KYC</p> <p>Businesses can be provided with hassle-free end-to-end fraud protection across their users' lifecycle, as well as ID verification via KYC checks. We address a large spectrum of fraud types, such as bot attacks, ATO, or chargeback fraud, and provide our clients with real-time actionable recommendations. What's more, we support our clients with:</p> <ul style="list-style-type: none"> <li>- more accessibility to fraud prevention by allowing them to choose and pay for only what they need from our modularised product.</li> <li>- first-hand darknet insights to proactively spot any fraud scheme that might reach out to their business</li> </ul>		
Technology			
	Native cloud		
Data input			
Identity verification	proprietary capability	third party	both
Personally Identifiable Information (PII) validation		x	
Small transaction verification	x		
Email verification			x
Phone verification			x
Social verification			x
Credit check		x	
Compliance check			x




Online authentication	proprietary capability	third party	both
Behavioural biometrics	x		
Device fingerprinting	x		
Geo-location			x
Remote access detection			x
3-D Secure 2.0		x	
Intelligence	proprietary capability	third party	both
Abuse list			x
Monitoring	x		
Address verification			x
Credit bureau		x	
Information sharing			x
Data ingestion/third-party data			
Stateless data ingestion and augmentation		x	
Methodology			
Machine learning	Hybrid		
Decisioning			
	Case management Decision orchestration		
Chargeback management			
	Chargeback dispute		
Business model			
Pricing model	Per transaction/operation and based on volume + fixed fee in some cases depending on the traffic		
Fraud prevention partners	Ekata, ComplyAdvantage, Assertiva, Verifi, Ethoca, Authologic, IP intelligence, BIN databases		
Year over year growth rate	Information available upon request.		
Number of employees	100+		
Future developments	Nethone KYC - risk-based approach to KYC New detection techniques of fraud tools Increased breadth and depth of Darknet research Modularized and tiered product offering that you can try for free straight from the website		
Customers			
Customers reference	Farfetch, Azul, Grupo Boticário, BlaBlaCar, VTEX, Grover, ZoodMall, Ramp, Nissho, Distributions, PLL LOT, Booksy, Wonga, ING, Forsh Commerce, Smartney, Carry1st		
	View company profile in online database*		
	*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a> .		

Nethone

# Protect your business from fraud during the entire user lifecycle



Company		Ping Identity	
		<p>Ping Identity is the Intelligent Identity solution for the enterprise. We provide flexible identity solutions that accelerate digital business initiatives, delight customers, and secure the enterprise through multi-factor authentication, single sign-on, access management, fraud prevention, intelligent API security, directory, and data governance capabilities.</p>	
Background information			
Year founded	2002		
Website	<a href="http://www.pingidentity.com">www.pingidentity.com</a>		
Target group	Merchants Marketplaces Banks/FS		
Supported regions	Global		
Contact	Divya Handa		
Member of industry association and/or initiatives	MRC, FIDO		
Core solution			
Core solution/problems the company solves	<p>Fraud and financial crime hub – decisioning platform            Account fraud            Digital identity service provider            Identity verification            Authentication</p> <p>Ping Identity’s fraud prevention solutions combine fraud monitoring, decisioning, ID verification, authentication, and orchestration tools to address fraud across the customer journey.</p>		
Technology			
	All, depending on solution: On-premise Cloud enabled Native cloud Hybrid		
Data input			
Identity verification	proprietary capability	third party	both
Identity document scanning	x		
Video scanning	x		
Personally Identifiable Information (PII) validation		x	
Email verification	x		
Phone verification	x		
Online authentication	proprietary capability	third party	both
Behavioural biometrics	x		
Physical biometrics	x		
Device fingerprinting	x		
Geo-location	x		
Remote access detection	Typically used for workforce – not consumer		
Mobile app push	x		

Hardware token	Typically used for workforce – not consumer		
One-time passwords	x		
Knowledge-based authentication	x		
<b>Data ingestion/third-party data</b>			
Stateless data ingestion and augmentation		x	
<b>Methodology</b>			
Machine learning	Rule-based Supervised ML Unsupervised ML Hybrid		
<b>Decisioning</b>			
	Decision orchestration		
<b>Chargeback management</b>			
	More information available upon request.		
<b>Business model</b>			
Pricing model	Pricing will depend on the collection of solutions that customers require to meet their use case.		
Year over year growth rate	23%		
Number of employees	1,232		
Future developments	We are working to augment our fraud detection capabilities to expand into further verticals. We are also continuously developing and releasing new integrations for third-party tools to ensure our customers can orchestrate solutions based on their existing technology mix.		
<b>Customers</b>			
Customers reference	<a href="https://www.pingidentity.com/en/customer-stories.html">https://www.pingidentity.com/en/customer-stories.html</a>		
	View company profile in online database*		
	*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a> .		

# Fight Fraud Trust Your Customers Grow Your Business



Ping Identity's intelligent fraud prevention solution detects fraud earlier in the user session and incorporates multiple threat signals to make automatic mitigation decisions in real time. It combines fraud detection, decisioning, ID verification, authentication, and orchestration tools on a single platform to address fraud across the customer journey and ensure legitimate customers do not feel the friction of fraud prevention.

## Detect

Detect bots and bad actors from the moment they interact with your digital properties, even before login.

## Decide

Aggregate multiple fraud signals into a single risk score and make fraud mitigation decisions.


## Direct

Deploy user journeys that integrate fraud prevention at key points throughout the session and send legitimate users down an easy path while challenging suspicious users.

## Defend

Deploy fraud mitigation methods that provide greater confidence in the identity and intent of users.

[Schedule a demo today to find out more](#)

Company		Riskified	
		<p>Riskified is on a mission to empower businesses to realise the full potential of ecommerce by making it safe, accessible, and frictionless. Leveraging machine learning that benefits from a global merchant network, our next-generation platform identifies the individual behind each online interaction, helping merchants eliminate risk and uncertainty from their business.</p>	
<b>Background information</b>			
Year founded	2012		
Website	<a href="http://www.riskified.com">www.riskified.com</a>		
Target group	Merchants/ecommerce		
Supported regions	US, Europe, APAC, LATAM, China		
Contact	<a href="mailto:hello@riskified.com">hello@riskified.com</a>		
Member of industry association and/or initiatives	Home Furnishings Association, IATA, MRC Global, AMVO, RILA, FinTech Australia, MAG		
<b>Core solution</b>			
Core solution/problems the company solves	<p>Card-not-present fraud, Friendly fraud, Account takeover, Policy abuse (refunds abuse, returns abuse, reseller/shipper abuse, promo abuse), Chargebacks disputes for all reason codes, Chargeback management, Payment optimisation, Direct debit fraud, BNPL fraud.</p> <p>Riskified helps companies grow their online business by reviewing and approving transactions while preventing fraud, preventing policy abuse, stopping account takeovers, and turning wrongly declined payments into revenue.</p>		
<b>Technology</b>			
	Native cloud		
<b>Data input</b>			
<b>Identity verification</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Personally Identifiable Information (PII) validation	x		
Email verification	x		
Phone verification	x		
Social verification	x		
<b>Online authentication</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Behavioural biometrics	x		
Device fingerprinting	x		
Geo-location	x		
Remote access detection	x		
Mobile app push	x		
One-time passwords	x		
<b>Intelligence</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Abuse list	x		
Monitoring	x		
<b>Data ingestion/third-party data</b>			
Stateless data ingestion and augmentation		x	

<b>Methodology</b>	
Machine learning	Supervised ML Unsupervised ML Rule-based
<b>Decisioning</b>	
	Decision orchestration
<b>Chargeback management</b>	
	Guaranteed fraud and friendly fraud protection, automatic chargeback dispute (all reason codes)
<b>Business model</b>	
Pricing model	Pricing is per transaction and based on volume for fraud and policy, with added flat costs for additional chargeback management capabilities
Fraud prevention partners	Our partner programmes are designed to give agencies, technology providers, and financial institutions access to our next-generation risk management platform so they can help their clients sell more and improve customer experience, while eliminating fraud. By combining our deep expertise in fraud management with our partner's established client engagement models, together, we enable ecommerce merchants to increase revenues by safely accepting more orders.
Number of employees	750+
<b>Customers</b>	
Customers reference	GoPro, Wish, REVOLVE, Finish Line, Agoda, The Level Group, Peloton, Canada Goose, Trip.com, Acer, Wayfair, Lastminute.com, Brooklinen, Steve Madden, Ring, Aldo, Air Europa, Giftcard.com, Movado Group, Prada, Farfetch, Swarovski, Geox, Megabus.com, Kiko Milano, eSky, MVMT
	View company profile in online database*
	*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a> .

Drive revenue, operational efficiencies  
and superior customer experiences with  
eCommerce fraud prevention



### Chargeback Guarantee

#### Raise approval rates

Eliminate 100% of chargeback costs



### Policy Protect

#### Reward loyalty

Block promo, reseller & refund fraud



### Account Secure

#### Build trust

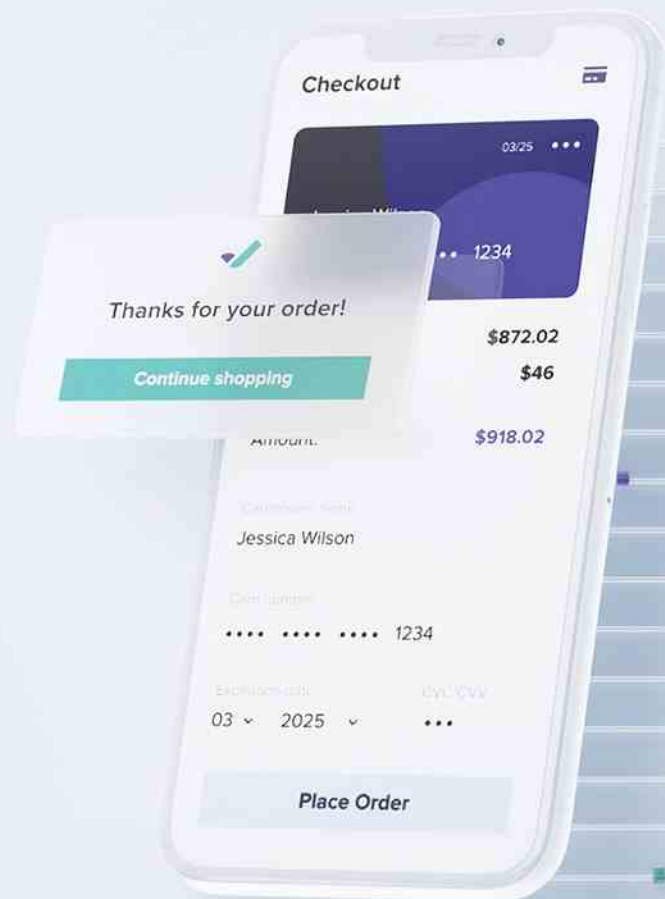
Protect your CX & the bottom line



### PSD2 Optimize

#### Maximize exemptions

Reduce risk & checkout friction



Transforming eCommerce for leading merchants and millions of worldwide consumers

**Trip.com**


**wayfair**

**ticketmaster**

**PRADA**

**wish**



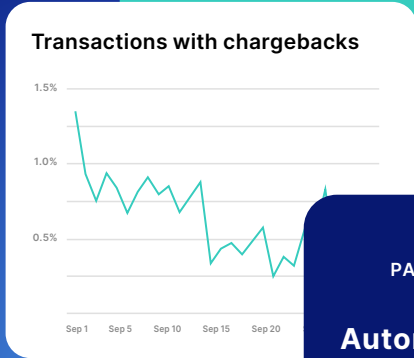
Company		Sift	
		<p>Sift is a leader in Digital Trust &amp; Safety, empowering digital disruptors and Fortune 500 companies to unlock new revenue without risk. Sift dynamically prevents fraud and abuse through industry-leading technology and expertise, unrivalled global data network of 70 billion events per month, and a commitment to long-term customer partnerships. Global brands such as Doordash, and Wayfair rely on Sift to gain a competitive advantage in their markets.</p>	
<b>Background information</b>			
Year founded	2011		
Website	<a href="https://sift.com/">https://sift.com/</a>		
Target group	Merchants/ecommerce (e.g. retailers, food & beverage, marketplaces, travel, gaming, etc.) Fintech PSPs		
Supported regions	Global		
Contact	<a href="mailto:sales@sift.com">sales@sift.com</a>		
Company's motto	Our mission: Help everyone trust the internet		
Member of industry association and/or initiatives	Marketplace Risk, Merchant Risk Council, Merchant Advisory Group, The Fraud Practice		
<b>Core solution</b>			
Core solution/problems the company solves	Digital Trust & Safety Platform for payment fraud Fake account detection Account take over Consumer authentication Content integrity Bot detection Chargeback management  Sift offers end-to-end fraud and risk mitigation solutions that secure each touchpoint of the customer journey.		
<b>Technology</b>			
	Native cloud		
<b>Data input</b>			
<b>Identity verification</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Small transaction verification	x		
Email verification	x		
Phone verification		x	
<b>Online authentication</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Physical biometrics	x		
Device fingerprinting	x		
Geo-location	x		
3-D Secure 2.0		x	
One-time passwords	x		
<b>Online authentication</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Information sharing	x		
<b>Data ingestion/third-party data</b>			
Stateless data ingestion and augmentation		x	

<b>Methodology</b>	
Machine learning	Supervised ML Unsupervised ML Rule-based
<b>Decisioning</b>	
	ML based decision engine Custom rule builder Decision orchestration Advanced link analysis with bulk decisioning Case management
<b>Chargeback management</b>	
	Chargeback dispute
<b>Business model</b>	
Pricing model	Per transaction based on volume and complexity
Fraud prevention partners	Adobe (Magento Commerce), Salesforce Commerce Cloud, Shopify, Wagento, Apruvd, Dwolla, CES, Olo, Checkout.com, Astound Commerce, Ekata, Macnica Networks
Year over year growth rate	Privately held
Number of employees	Privately held
Future developments	Privately held
<b>Customers</b>	
Customers reference	Box, McDonald's, Wayfair, Coinjar, Twilio, Uphold, Poshmark, Patreon, Reddit, Remitly, Hello Fresh, Traveloka
	<a href="#">View company profile in online database*</a>
	*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a> .



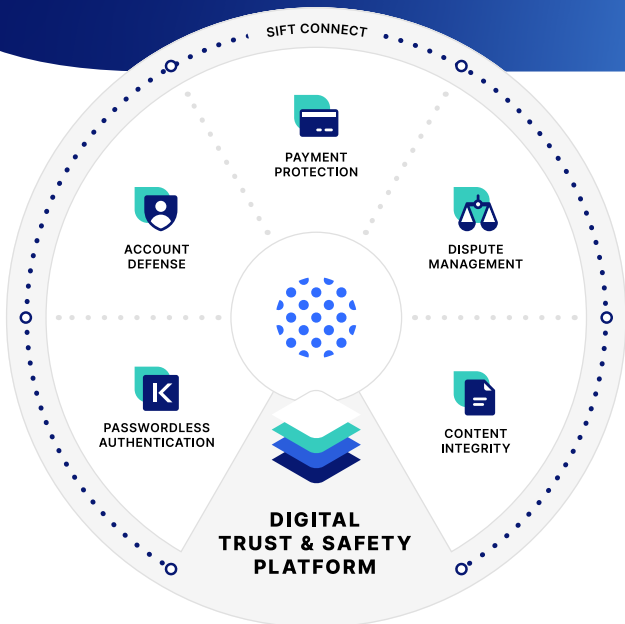
# Cut fraud losses by 90%

Proactively stop fraud and fuel growth from login to chargeback with the Digital Trust & Safety Platform.




**PAYMENT PROTECTION**

**Automate on-demand authentication**



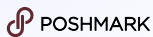
## A smarter, simpler way to stop fraud

Built with a single, intuitive console, Sift’s end-to-end solution eliminates the need for disconnected tools, single-purpose software, and incomplete insights that drain operational resources.


The Sift Digital Trust & Safety Platform does what other fraud tools can’t, adding connected data, adaptability, and intelligent automation to every aspect of risk operations.

## Leading brands rely on Digital Trust & Safety

Launch unbeatable defenses against current and future threats using accurate, real-time data from our global network of 70B events per month, representing 34K sites and apps.



Visit [sift.com](https://sift.com) to learn more →

Company		Signifyd	
		Signifyd empowers fearless commerce by providing an end-to-end Commerce Protection Platform that protects merchants from fraud, consumer abuse, and revenue loss caused by friction in the buying experience.	
Background information			
Year founded	2011		
Website	<a href="http://www.signifyd.com">www.signifyd.com</a>		
Target group	Merchants/ecommerce PSP/acquirers Banks/FS Corporate Fintech Telecom		
Supported regions	Global		
Contact	Amal Ahmed, Head of Global Financial Services and EMEA Marketing		
Company's tagline	Fearless Commerce		
Member of industry association and/or initiatives	MRC, BRC, IMRG, FIDO, Vendorcom		
Core solution			
Core solution/problems the company solves	Fraud/risk management and decisioning platform Customer authentication Identity verification Behavioural biometrics Data provider and intelligence Chargebacks management Bot risk management KYB/Merchant onboarding KYC  Signifyd is the largest provider of commerce protection with a network made up of thousands of ecommerce merchants, including two of the top three largest retailers globally. Signifyd optimises merchants' revenue with a unique combination of identity and intent intelligence, machine learning, and domain expertise to address all chargeback types and to ensure that legitimate orders are never falsely declined. Signifyd demonstrates its trust in its decisions with a 100% financial guarantee for approved orders that result in fraud or abuse chargebacks.		
Technology			
	Native cloud		
Data input			
Identity verification	proprietary capability	third party	both
Personally Identifiable Information (PII) validation	x		
Email verification	x		
Phone verification	x		
Social verification	x		
Compliance check	x		

Online authentication	proprietary capability	third party	both
Behavioural biometrics	x		
Physical biometrics	x		
Device fingerprinting	x		
Geo-location	x		
Remote access detection		x	
Mobile app push	x		
3-D Secure 2.0	x		
Hardware token	x		
Knowledge-based authentication	x		
Intelligence	proprietary capability	third party	both
Abuse list	x		
Monitoring	x		
Address verification	x		
Information sharing	x		
Data ingestion/third-party data			
Stateless data ingestion and augmentation		x	
Methodology			
Machine learning	Supervised ML Unsupervised ML Hybrid		
Decisioning			
	Case management Decision orchestration		
Chargeback management			
	Chargeback dispute Guaranteed fraud protection		
Business model			
Pricing model	Signifyd's pricing model depends on the specific capabilities licensed by its customers and ranges from flat fee, to transaction-based pricing, to percentage-of-GMV pricing.		
Number of employees	500+		
Customers			
Customers reference	Samsung, eBay, Emma, Illy, Mango, Huda Beauty		
	View company profile in online database*		
	*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a> .		

# Where every transaction matters

## ONE PLATFORM BUILT TO MAXIMIZE PAYMENT CONVERSIONS

Signifyd's Payments Optimisation Platform helps payment providers retain existing merchants and win new business by offering value added services beyond their existing offerings. Built to fearlessly authorize more payments and deliver decisions that are backed by a financial guarantee, the platform is underpinned by the largest enterprise network on the market to identify the shopper behind 98% of online purchases.



### Increase revenue

With the largest enterprise merchant network on the market, Signifyd can help grow your revenue and merchant retention through a 5-9% increase in approvals.



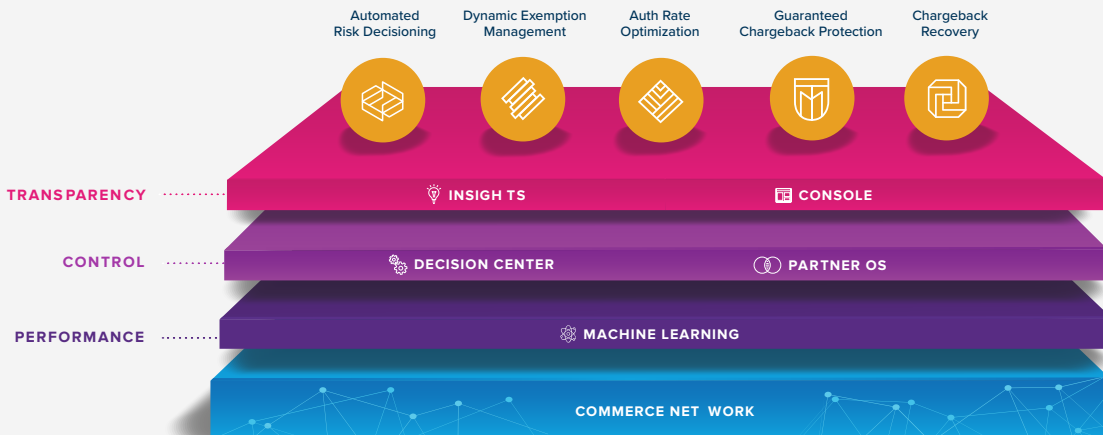
### Retain and grow your merchant base

Whitelabel and resell value-added services for new revenue streams to expand your business and retain existing merchants.



### Reduce operational costs and fees

Leverage Signifyd's automated fraud decisioning and chargeback recovery tools to reduce operational costs and fees.




“As the global ecommerce market continues to grow and payments and checkout needs become more complex, merchants require more sophisticated solutions to optimize transactions acceptance while protecting commerce.

We are continually impressed with Signifyd's innovative approach to this market need and our partnership with them has helped us unlock better experiences for both our merchants and their shoppers.”

– JIM JOHNSON, HEAD OF MERCHANT SOLUTIONS AT FIS

**worldpay**  
from FIS



Company		Worldline	
		<p>Worldline is the European leader in the payment and transactional services industry. With innovation at the core of its DNA and thanks to a presence in 30+ countries, Worldline is the payment partner of choice for merchants, banks, public transport operators, government agencies, and industrial companies, delivering cutting-edge digital services.</p>	
<b>Background information</b>			
Year founded	1973		
Website	<a href="https://worldline.com/en/home.html">https://worldline.com/en/home.html</a>		
Target group	Merchants/ecommerce Banks/FS Corporate Fintech Telecom		
Supported regions	Europe		
Contact	Claire DEPRESZ-PIPON – <a href="mailto:claire.pipon@worldline.com">claire.pipon@worldline.com</a>		
Company's motto	Digital payments for a trusted world		
Member of industry association and/or initiatives	EMVCO, W3C, FIDO Alliance, EDPIA, EPI		
<b>Core solution</b>			
Core solution/problems the company solves	Customer authentication Behavioural biometrics We offer a multi-factor authentication solution that brings security to all sensitive operations (payment, online banking, digital identity, etc.). This solution is combined with different fraud detection assets which prevent intrusion and attacks.		
<b>Technology</b>			
	Cloud-enabled		
<b>Data input</b>			
<b>Online authentication</b>	<b>proprietary capability</b>	<b>third party</b>	<b>both</b>
Behavioural biometrics			x
Physical biometrics		x	
Device fingerprinting	x		
Geo-location	x		
Remote access detection		x	
Mobile app push	x		
3-D Secure 2.0	x		
Hardware token		x	
One-time passwords	x		
Knowledge-based authentication	x		
<b>Methodology</b>			
Machine learning	Rule-based Supervised ML Hybrid		
<b>Decisioning</b>			
	Manual review Case management Decision orchestration		

Business model	
Pricing model	Transaction-based pricing model
Fraud prevention partners	Internal capabilities + inform Riskschield
Year over year growth rate	For business revenues, please refer to our corporate investor page <a href="https://investors.worldline.com/en/home.html">https://investors.worldline.com/en/home.html</a> Yearly growth: 80%
Number of employees	20,000+
Future developments	For more details, please contact our sales team.
Customers	
Customers reference	For more details, please contact our sales team.
	View company profile in online database*
	*The data present at the time of publication might be subject to changes and updates. For the latest stats and information, we invite you to check the profile in our <a href="#">online company database</a> .





## How to optimise **user experience** while ensuring a high level of **security**?



**In 2022**

**+500M**

strong authentications

**+2B**

3DS transactions



**Seamless authentication method**



**Adaptable to your digital strategy**



**Data collection for intelligent scoring**

## Don't Miss the Opportunity of Being Part of Large-Scale Payments Industry Overviews

Once a year, The Paypers releases six large-scale industry overviews covering the latest trends, developments, disruptive innovations, and challenges that define the global online and mobile payments, e-invoicing, B2B payments, ecommerce, and web fraud prevention and digital identity space. Industry consultants, policy makers, service providers, and merchants from all over the world share their views and expertise on different key topics within the industry. Listings and advertorial options are also part of the guides for the purpose of ensuring effective company exposure at a global level.



Payment Methods Report  
2022



Cross-Border Payments  
and Ecommerce Report  
2022-2023



Crypto Payments and  
Web 3.0 for Banks,  
Merchants, and PSPs Report



Who's Who in Payments  
Report 2022

For the latest edition, please check the [Reports section](#)

