



Fraud Prevention in Ecommerce Report 2020/2021

The Ultimate Source in Securing Transactions While Offering
a Frictionless Journey to Customers

Endorsement partners:



THEFRAUDPRACTICE

Key media partners:



Fraud Prevention in Ecommerce Report 2020/2021

The Ultimate Source in Securing Transactions While Offering
a Frictionless Journey to Customers

Contact us

For inquiries on editorial opportunities please contact:

Email: editor@thepaypers.com

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

For general advertising information, contact:

Mihaela Mihaila

Email: mihaela@thepaypers.com



RELEASE VERSION 1.0

NOVEMBER 2020

COPYRIGHT © THE PAYPERS BV

ALL RIGHTS RESERVED

TEL: +31 20 893 4315

FAX: +31 20 658 0671

MAIL: EDITOR@THEPAYPERS.COM

Management Summary

Besides looking at the current state of affairs in the commerce industry and checking the emerging fraud threats that risk management teams are dealing with, via the 2020/2021 edition of this Report we aimed to depict valuable views into fraud detection and risk management; new methods of leveraging artificial intelligence and machine learning; and the impact of PSD2's SCA. This is our way to help players in the payments space to keep pace with the latest trends and developments, fraud challenges, the newest technologies to combat fraud attacks, and the upcoming regulations.

Current state of affairs

In 2020, the industry players have faced quite a bumpy ride so far: not only has the COVID-19 impact been felt by all industries, but both businesses and consumers have had to shift the move to digital transactions.

There has been a rapid switch towards digital payments, and customers' preferences have definitely been impacted. We can now see more and more cashierless pay points and retailers that offer various benefits via mobile apps, which streamline consumers' experience. In its **Cybercrime Report**, for instance, LexisNexis Risk Solutions reveals that mobile device transactions continue to rise, with 66% of all transactions coming from mobile devices in H1 of 2020.

In July 2020, a survey conducted in the **UK** regarding shopping behaviour found that 63% used more electronic payments as a result of COVID-19, while the same percentage used more card payments in general, and 80% used more contactless card payments.

What is worrying here is the fact that fraudsters are opportunistic, and they will always look for weak loopholes to achieve their goal. So, as ecommerce has risen and fraudsters take advantage, now more than ever everyone needs to be informed and to act efficiently. How can this be attained?

With three main steps:

1. Knowing the enemy;
2. Knowing the challenge;
3. Knowing the solution.

Keep your friends close and your enemies closer

This boost in ecommerce brought along new groups that were basically urged to adapt to digital transactions: senior consumers, minor generations, and brick and mortar merchants that had to open up online channels quickly during the lockdown. All these groups are on the list of those most vulnerable. Consumers, in their digital journey, experience high rate attacks in new account creations, yet the largest volume of attacks target online payment transactions, according to LexisNexis Risk Solutions.

Besides the rise of online shopping, Buy Online, Pickup In Store (BOPIS) is another method consumers have adopted, especially during the pandemic, as per the **National Retail Federation**. This buying trend is referred to as 'Click-and-collect' within non-US geographies. However, Kount reports that fraudsters are taking advantage of this shopping trend, as they steal and use credit cards and account credentials, pick-up the goods in-store, and afterwards keep the item for themselves or resell it. After all, *'Fraudsters go where the money and data are, and they know digital experiences are a prime opportunity'*, as Rich L. Stuppy, Chief Customer Experience Officer at Kount, states. The reason why BOPIS is such an easy target is the fact that it requires minimal proof of purchase, so bad actors **'get in and out without detection'**. →

Management Summary

In addition, if we consider fraudster's business model during this lockdown period, we can see that bad actors turn to several attack typologies such as account takeover (ATO) attacks using identity spoofing and chargeback fraud. In fact, Breach Clarity argues that retailers are the most heavily targeted industry segment for credential stuffing attacks that can lead to ATO. Typical merchants do not always deploy stronger forms of authentication than organisations like financial institutions do. A solution would be for strong authentication to become more the norm than the exception; however, until then, Al Pascual from Breach Clarity believes that 'fraudsters armed with compromised credentials will drive ATO higher among ecommerce merchants'.

In January, Javelin released its **Protecting Digital Innovation: Emerging Fraud and Attack Vectors** report, which emphasises that CNP fraud and account takeover are top fraud threats for merchants, with 34% and 24% respectively. However, one must take into account that although ATO is harder to detect, it is easier to commit for fraudsters.

Why merchants don't have an easy road

Javelin suggests that many merchants choose to simplify the checkout process and consumers are enabled to create an account and save their payment information. Once the data is stored in the merchant's systems, the merchant actually places themselves at **a higher risk for fraud**. The report unveils that nowadays criminal organisations can attack a wide range of targets with tactics like social engineering and automated credential stuffing, which allow them to defeat rudimentary defences. However, one solution that could make this process safer is through the use of tokenization, which is the process of turning an important piece of data (e.g. an account number) into a random string of characters called a token that has no meaningful value if breached.

Alasdair Rambaud from SecuredTouch talks about the fact that businesses face no-transaction fraud. Although this type of fraud doesn't result in a direct purchase via a checkout process, it can cause substantial damage to the business and it is hard to detect. Such fraud includes activities like refund requests for goods not actually purchased, coupon fraud where coupon codes are maliciously obtained and used or sold loyalty and reward fraud. The fraudsters' gain from stealing personally identifiable information (PII) is major as it can either result in identity theft or stolen credentials that are further used in other websites/apps or sold to other malicious actors.

Marqeta's 2020 Fraud Report, *Why consumers don't understand card fraud*, surveyed 4,000 consumers across the US and the UK and discovered that 42% had been hit by fraudsters. 87% admitted they would agree for transactions to take longer to complete, if extra steps for authentication meant their information was better protected. However, while this need is perfectly understandable, it is not that easy to get there. To implement extra authentication steps means data dependency and collaboration between acquirers, merchants, and issuers. And optimising a data sharing scheme along with the customer journey while employing the best risk modelling process is not simple.

Moreover, the upcoming PSD2 with its Strong Customer Authentication (SCA) is aimed at consumer protection and making ecommerce safer. Although PSD2 was to go into effect on 14 September 2019, the European Banking Authority (EBA) granted additional potential exemptions and set the new **deadline to 31 December 2020**. The fact that there will be further exemptions and out of scope transactions only means that fraudsters will have more options to exploit.

Kurt Schmid from Netcetera believes that '[...] if the right technologies are used and processes are optimised, the requirements of PSD2 and Strong Customer Authentication can be met without jeopardising conversion and without having to fear revenue loss'. The question is: are businesses ready? One aspect that merchants can take into account, for instance, is to check out for companies that offer FIDO authentication within their solutions. Nok Nok Labs is a company that provides a FIDO-based solution which replaces 'passwords with secure and simple authentication measures such as fingerprint and device ID' and which complies with regulations like PSD2 SCA. Walter Beisheim from Nok Nok highlights why it is important to deliver consistent and secure SCA, and how this can help and benefit merchants. →

Management Summary

Finding if every door has a key – the ‘challenge accepted’ game is on

As fraud becomes more sophisticated and as fraudsters obtain access to the latest technology and tools, the question that raises is *what can be done?* Have we used the current techs to the maximum or should we look into new technologies? If we need to search for new ways and tools for protection, what are those? What is certain is that consumer education is a must and they should stay informed regarding both the risks and the ways to prevent any activities from fraudsters.

While innovations are taking place in the fraud technology space, it is interesting to see how artificial intelligence and machine learning have been evolving. As such, STRATGranat teaches us that an automated machine learning allows the manual review team and fraud manager to manage alerts triggered by the machine learning if there are spikes in decisions not previously seen. In addition, Simility stresses upon the fact that the use of explainability methods allow businesses to gain vital insight into the whole process, from data collection to decision making.

On the other hand, it can be difficult for merchants to test and evaluate the best innovative fraud solution. Why? Because *‘no two merchants are exactly the same’*, and what they sell, what their customers are or what fraud challenges they have been all part of what makes their needs unique. Testing can be expensive and outperforming an incumbent solution can be challenging. For this reason, Insparx talks about solutions that are available in payments and how a single API in the fraud orchestration hub can be benefic.

In addition, Mango, like many other merchants, has seen huge spikes in their online channels, as they had to deal with more Internet traffic and to offer new customer journeys. However, with the transition towards digital channels, merchants also face an increase in fraud attempts such as BOPIS, BOPAC, ATO, or chargebacks. So as fraudsters try to steal credentials from legitimate customers, Mango talks about their learnings and best practices on how to focus on good customers, while blocking bad ones.

At the same time, merchants need to detect fraud during the entire customer journey, ‘not just at the time of financial transaction’, as Patrick Finnigan from Dunkin’ Brands suggests. However, businesses new to digital commerce struggle because some have not invested in solutions for the risks associated with the mobile and online channels. Dunkin’ Brands gives a piece of advice on what can businesses do to choose the best protective measures. After all, merchants’ goal is to protect their revenue, customer’s data, and the reputation of one’s brands, isn’t it?

As such, to picture the newest technologies, the final part of the Fraud Prevention in Ecommerce Report 2020/2021 focuses on mapping the key players in the fraud detection, identity verification, and online authentication area, as well as presenting their backgrounds and features via in-depth profiles. The chapter aims to reveal an overview of the solution providers in the fraud prevention space and the most important capabilities of each company, thus helping merchants, fintechs, and payment service providers to grasp the current market opportunities.

We would like to express our appreciation to the Merchant Risk Council, Marketplace Risk, and Fraud Practice – our endorsement partners who have constantly supported us – and also to our thought leaders, participating organisations, top industry players, experts, solution providers, merchants, industry associations, and consultancy companies that contributed to this edition. They’ve enriched our report with their valuable insights and joined us in our never-ending journey to depict an accurate overview of the industry.

Enjoy your reading!

Simona Negru | Content Editor | The Paypers

Table of Contents

3	Management Summary
8	The Current Landscape and Emerging Fraud Trends in Commerce
9	How Is the Ecommerce Space Influenced by the Pandemic? Kevin J. Sprake, Managing Partner, The Fraud Practise
11	COVID Brings an Explosion in Ecommerce, but High Volume of Stalled Carts Causes Concern Gerhard Oosthuizen, CTO, Entersekt
13	Post-Pandemic: Focus on Evolving Fraud & Cyber Strategies – Learning from the Wirecard Scandal Neira Jones, Ambassador, EPA
15	Challenges in Ecommerce
16	Interview With ACI on Managing Fraud Successfully When Navigating the Digital Shift Fabian Gloerfeld, Head of Payments Intelligence, ACI Worldwide
18	Understanding True Intent: Probabilistic vs Deterministic Kevin Gosschalk, CEO and Founder, Arkose Labs
20	The Growing Popularity of No-Transaction Fraud Alasdair Rambaud, CEO, SecuredTouch
22	Merchants Need to Be a Mastermind in Today's Ecommerce World Ronald Praetsch, Co-Founder, About-Fraud
24	How the Pandemic Will Feed an Account Takeover Explosion Al Pascual, COO and Co-Founder, Breach Clarity
26	Tackling Fraud Challenges in Ecommerce Patrick Finnigan, Director of Loss Prevention Analytics and Fraud, Dunkin' Brands
28	Fighting Online Merchant Fraud Must Be Done Globally and Is Essential to Keep Trust in Online Payment Jorij Abraham, Managing Director, Ecommerce Foundation – Scamadviser
30	Interview With Mango on Known and Emerging Fraud Trends in Retail Carlos Madrona Guillén, Internal Control & Compliance, Payment Methods and Fraud Director, Mango
32	Hidden Frauds That Translate Into Marketplace Losses Jeremy Gottschalk, CEO, Marketplace Risk
35	Deceptive Counterfeiting: Criminals Defrauding Legitimate Consumers Shaun Packiarajah, Intelligence Analyst, React
37	Entrepreneurship and Merchant Fraud in a Post-Pandemic World Angie Dobbs, Director, Fraud & Risk, Wave Financial
39	Technologies and Innovations That Keep Fraudsters at Bay
40	Staying Ahead in a Changing World: Building Fraud Strategies That Get More Business In Mark Strachan, EMEA Managed Risk Principal, Cybersource
42	Interview With Fraugster on Best Practices on How Businesses Can Increase Approval Rates Max Laemmle, Founder & CEO, Fraugster
44	Three Keys to Protect and Scale Ecommerce In 2021 Rich L. Stuppy, Chief Customer Experience Officer, Kount
46	Interview With Sift on the Importance of Control and Transparency for Digital Trust & Safety Kevin Lee, Trust and Safety Architect, Sift
48	Why Explainability Is Key to Success in Machine Learning Sean Nierat, Product Marketing Manager, Simility, a PayPal Service
50	The Problems With the Fraud Proof of Concept and a Possible Solution Liam Castagna, Head of Payment, Insparx
52	Automation: An Enabler to Run a Marathon or Sprint Catherine Tong, Independent Fraud, Risk, and Payment Specialist, STRATGranat
54	AI-based Intelligent Verification and Authentication Are Coming Ralph A. Rodriguez, Executive-in-Residence, Summit Partners

Table of Contents

56	Overview of Key Industry Players
57	Mergers & Acquisitions in the Fraud Prevention Space – the Last 12 Months Overview Simona Negru, Content Editor, The Paypers
62	Solution Providers – Mapping of Core Features and Capabilities
77	The Impact of SCA Implementation – Now and After
78	MRC Advocates Extension as SCA Enforcement Deadline Approaches Julie Fergerson, CEO, Úna Dillon, Managing Director, MRC
81	COVID-19, PSD2, and the Consequences for Payments-21 Kurt Schmid, Marketing & Innovation Director Secure Digital Payments, Netcetera
83	Interview With Nok Nok on the Importance of Secure SCA in Mobile Apps and Browsers Walter Beisheim, Chief Business Development Officer, Nok Nok
85	The Upside Of 3DS 2 Implemented Well? 5%+ More Revenue Ed Whitehead, Managing Director, Europe, Signifyd
87	The Future of Fraud after PSD2's Strong Customer Authentication Deadline Jonathan Williams, Independent Advisor, MK2 Consulting
89	About Fraud and Strong Customer Authentication – Old Challenges, New Patterns Elena Emelyanova, Senior Payments and Fraud Manager, Wargaming
91	Company Profiles



The Current Landscape and Emerging Fraud Trends in Commerce

The impact of COVID-19 this year has been felt massively in the industry. Digital transactions and online channels have become a must during the pandemic. However, the downside is that fraudsters see this as an opportunity to explore further and online fraud has become a blind side of the ecommerce surge. Via this chapter, we have gathered insights regarding the known and emerging fraud trends amid coronavirus.

The Fraud Practice

How Is the Ecommerce Space Influenced by the Pandemic?



About Kevin J. Sprake: He is a veteran ecommerce payments and fraud prevention executive who is passionate about serving customers. He is a past-Global Board member of the Merchant Risk Council, and was recently named as the Managing Partner of The Fraud Practice.

Kevin J. Sprake ■ *Managing Partner* ■ The Fraud Practice

As the New Year begins and ecommerce sales are being tallied against fraud losses, ecommerce merchants, acquirers, solution providers, and issuers are typically preparing their lists for what worked and what didn't work as part of the Holiday Season. This year started in the same way but with one significant exception when undertones of an unknown virus expected to spread across the world became a harsh reality. COVID-19 was officially declared a 'global pandemic' on 11 March 2020 and organisations around the world quickly shifted their focus to emergency systems and operational planning to prepare for millions of workers to work from home, or sadly, to be removed from their jobs completely.

This black swan event set the stage for an abrupt and unanticipated explosion of ecommerce transaction volumes that will be studied and written about for years to come. The exodus of brick-and-mortar retail led to an acceleration of mobile and ecommerce growth, while organisations accelerated years of digital transformation in just a few months. The US Census Bureau recorded a 44.5% year-over-year increase in ecommerce retail sales during the second quarter of 2020.

As quickly as card-present and omnichannel merchants moved to revise their business plans to support ecommerce models and implement curbside pick-up procedures, the fraudsters went to work using an old playbook that was proven and very effective. The increased volume of online and mobile transactions, heightened by the panic of a global pandemic, left the door wide open for the all too familiar scams that supported huge spikes in identity theft, account takeover, and ultimately third-party and application fraud.

Early on, COVID-19 perpetuated a level of real fear in most people that can create an emotional and debilitating physical response, often leading to the use of poor judgment in stressful situations. This environment exposed a vulnerability that allowed phishing schemes to be highly effective as people literally feared for their lives.

There is a saying used in risk mitigation and fraud prevention that says: 'follow the money and that will show you the open door'. When the US Government approved the Cares Act and trillions of dollars were being disbursed to millions of Americans, it was not clearly understood how the disbursement process would work and the confusion led to large scale targeted phishing attacks. Phishing schemes also targeted consumers who wanted to purchase masks, hand sanitizer, and other essentials suddenly in short supply. For years fraudsters have taken advantage of consumers and increased the number of phishing scams used to extract a person's credentials, but it was the added fear of COVID-19 and the impact of shelter in a place that made the scams even more effective. Google identified a 250% increase in phishing sites between January and March.

Another opportunity for fraudsters came in the form of Business Email Compromise (BEC) attacks. Many organisations went from few or no employees working remotely, to their entire workforce working at home. Fraudsters pounced on the chance to exploit less secure hardware and security practices in the home, as well as the physical distance from IT and cybersecurity teams. →

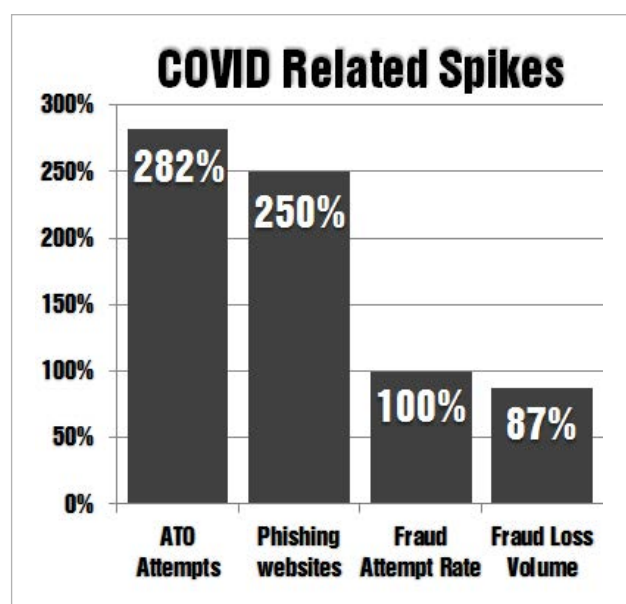
Fraudsters used social engineering to obtain information to bypass two-factor authentication measures, then took over the email accounts of unsuspecting employees and executives, and used the trust associated with these email accounts to reroute payments and access additional personally identifiable information.

Businesses were being attacked on multiple fronts. Direct attacks including data breaches, social engineering, and Business Email Compromise had all greatly increased. Meanwhile, businesses also experienced a surge in online and mobile commerce from both legitimate consumers and fraudsters leveraging compromised consumer payment account and identity credentials. The behaviour of a typical consumer drastically changed at the same time fraudsters ramped up their activity. Historical patterns that previously would've been recognised as a high risk or a typical fraud event, were no longer as clear. It became extremely difficult for organisations to discern a true fraud attack from what was becoming the 'new normal'. Businesses felt the impact in terms of more fraud losses, higher decline and false-positive rates, and increased chargebacks related to fulfilment and other non-fraud reasons.

Typically, the victims of online fraud are unsuspecting individuals who are vulnerable because of their age, technical ability, and lack of knowledge about fraud scams. According to the Federal Trade Commission, Americans have already lost more than USD 145 million to fraud related to the coronavirus, measured by more than 200,000 complaints from consumers. The full residual impact globally is yet to be known, but rest assured that the numbers will be significantly higher. As personally identifiable information, collected through the various schemes discussed, is used over the holiday to perpetrate more fraud against merchants, the victims of

COVID-19 will extend beyond the consumer to included merchants, acquirers, and issuers.

It is difficult to put history into words, especially as we are living through it, but the pandemic has influenced ecommerce in a way that will change how we think about everything going forward. The way we work, shop, learn, and the way we interact with one another will forever be changed.



About The Fraud Practice: A payments and risk focused consulting firm that leverages their global market experience to work with merchants, financial institutions, and service providers to assess, design, improve, and bring to market new solutions in ecommerce. Since 2004, their assessments and strategies have helped customers to re-define the fraud and payments industry.

www.fraudpractice.com

Entersekt

COVID Brings an Explosion in Ecommerce, but High Volume of Stalled Carts Causes Concern



About Gerhard Oosthuizen: As CTO, Gerhard is responsible for accelerating strategic initiatives at Entersekt, driven by innovation as well as research and development. He has over 20 years' experience in the software industry, developing and managing software across the globe.

Gerhard Oosthuizen ■ CTO ■ Entersekt

While many businesses have floundered during the pandemic, the regulatory response has created an environment for tech companies to flourish. Unsurprisingly, in a time of lockdown and restrictions, ecommerce has boomed. According to Adobe, online shopping in the United States **achieved between four and six years' worth of growth** in just a couple of months earlier this year. April and May saw more online spend than the 2019 holiday season, by far the most important six or so weeks in American retail.

Experience tells us that once a customer successfully downloads and uses an ecommerce app, they are unlikely to return to their previous method of transacting. The convenience of using the app helps to convert the unsure and undecided.

Obstacles remain, however, and there is a high rate of transaction failure. To sustain growth, we need to understand and solve the challenges that lead to incomplete transactions. As pandemic restrictions are lifted and people can move more freely, their shopping options will increase, which means a higher rate of people than usual may shift back to previous transaction habits.

There is an urgency, therefore, to understand and solve ecommerce's biggest obstacles.

User experience is key

An obvious but crucial point is the importance of user experience. The modern digital consumer expects sophisticated, slick, and safe user experiences, accessible anytime, anywhere, and on any device.

It seems, however, that many experiences are falling short. Consider these **numbers from Ethoca:**

- nearly two-thirds of abandoned carts (65%) occur because of friction;
- due to fraud controls, USD 146 billion in card-not-present purchases are declined each year;
- yet of these transactions, more than half (52%) were not fraudulent.

These are significant numbers and represent a substantial loss of sales valued around USD 100 billion every year. Losses are probably considerably more, however, as after a card is declined, 64% of customers will abandon the transaction, and 80% will tell a friend about their negative experience.

An enhanced, elegant user experience, one that engages the customer and helps to solve any issues that arise during the transaction, is required. Several operators are currently working towards a solution, but as they tend to differ on their definition of the problem, routes vary.

Let's examine the different options.

All roads lead to Rome; some will get you there quicker

EMVCo, the global technical body that facilitates worldwide interoperability and acceptance of secure card payment transactions, along with the payment networks, champions three options:

• Tokenization

By converting sensitive cardholder information into a unique digital identifier, this creates a token that can then be used instead of a card, which helps to protect the primary account numbers. A unique number is provided for each environment, and the card number is limited. →

Should the token be fraudulently acquired, it can only be used for the intended recipient. Tokens can be issued either through an issuer wallet, a third-party wallet or a card-on-file.

• 3-D Secure

3-D Secure is an authentication vehicle, a messaging protocol that enables issuers to authenticate consumers during online shopping. It provides a layer of security that reduces fraudulent transactions, prevents unauthorised use of credit and debit cards online, and protects merchants from exposure to fraud-related chargebacks.

• Click to Pay

A relatively recent rollout by EMVCo, card information is secured on the users' profile who can then choose which card they want to use for the transaction as they would in a real-world situation, with no need to enter a password or card details. Click to Pay aims to offer a simple, seamless, and safe user experience that saves the customer time. The interface is standard across the web and mobile sites, apps, and devices.

Other operators and options include:

• Payment Request API

The Web Payments Working Group (WPWG) consortium controls the standards of payments across the internet. With its Payment Request API, the WPWG aims to standardise communication across merchants, browsers, and payment methods by providing a single, stable, and consistent API for developers. Merchants can create a controlled and standardised checkout experience for all payment types, not just card payments.

• FIDO with WebAuthn

Entersekt, along with Microsoft, Google, Amazon, and Facebook, belongs to the FIDO Alliance, which stands for Fast Identity Online. We have long supported its drive to banish inconvenient and weak password-based security, and we expect to see a rapid surge in interest following a recent announcement by Apple that it will fully support the new FIDO2 authentication protocol too.

The way forward: cooperation and collaboration

The most significant potential lies in collaboration, and we see the beginning of alliances between groups, such as the relationship between the World Wide Web Consortium (W3C) and FIDO to enable WebAuthn. There is also a W3C, FIDO, and EMVCo working group that is currently discussing, allowing merchants to submit FIDO tokens.

However, while there is overlap, and operators are talking to each other about common ground, specifications remain quite varied. Banks and merchants may struggle to understand which options work well together and are best suited to their needs. It will require expert knowledge of the market, the various solutions, and the future of ecommerce, and it is best to work with a specialist.

About Entersekt: Entersekt is a leading provider of device identity and customer authentication solutions. Its multi-patented, regulatory compliant technology helps financial institutions and other enterprises to build trust and boost loyalty with secure, convenient, and engaging new digital experiences.

www.entersekt.com

[Click here for the company profile](#)

Post-Pandemic: Focus on Evolving Fraud & Cyber Strategies – Learning From the Wirecard Scandal



About Neira Jones: Neira advises organisations on many topics, including payments, fintech, regulations, and cybersecurity. She is also a professional speaker, regularly addressing global audiences, and is a recognised trainer (see her on-demand e-learning courses [here](#)).

Neira Jones ■ Ambassador ■ EPA

When I wrote my **last post** for The Paypers, the world was a very different place. The pandemic has upturned the way we live and the way we do business, and its effects will be lasting, not least the extraordinary surge in adoption of digital services. As consumer behaviours drove the need for access to financial services without having to handle cash or other ‘unsafe’ payment methods, financial services companies were only too happy to oblige, and fintech popularity increased as a result. The demand for digital services led to even more dependencies on the digital supply chain, leading many to wonder what effect a massive supply chain failure would have on the payments industry. We didn’t have to ponder for very long.

Reading the signs

In January 2019, a **Financial Times investigation** highlighted underlying problems with potentially false accounting and money laundering in the Asian operation of Wirecard. Questionably, Edo Kurniawan, the accountable executive, remained in position after the investigation showed numerous accounting and internal controls failures for more than a decade. Subsequent clean audits from EY gave Wirecard a semblance of respectability. As expected, Wirecard played the **deflection** card when the FT contacted them, affirming that it ‘took all compliance and regulatory obligations extremely seriously’, and that it had ‘stringent internal and external audits’, and that any concerns were ‘always thoroughly and appropriately investigated’. It then became apparent that Wirecard **processed transactions for a Maltese Mafia-linked casino**, known for its money laundering activities. Analysts, investors, and regulators, with few exceptions, largely turned a blind eye. Wirecard ex COO is now on **Interpol’s most wanted list** and **its assets are being sold off**.

The consequences were stark: this **fintech success story** turned into a nightmare and Wirecard was suspended by several regulators, leaving many of their **fintech customers unable to process payments**. This left consumers, some in vulnerable segments, unable to access their fund.

As this most epic governance failure unfolded, it was a clear reminder that even in times of crisis, businesses must not relax their governance and risk postures in order to continue protecting consumers’ data and assets.

Don’t pass the buck

Some blamed the regulators, arguing that existing frameworks were not adequate. It is my firm belief that regulations are no substitute for accountability, transparency, governance, and risk management. Let’s not repeat the Wirecard mistakes:

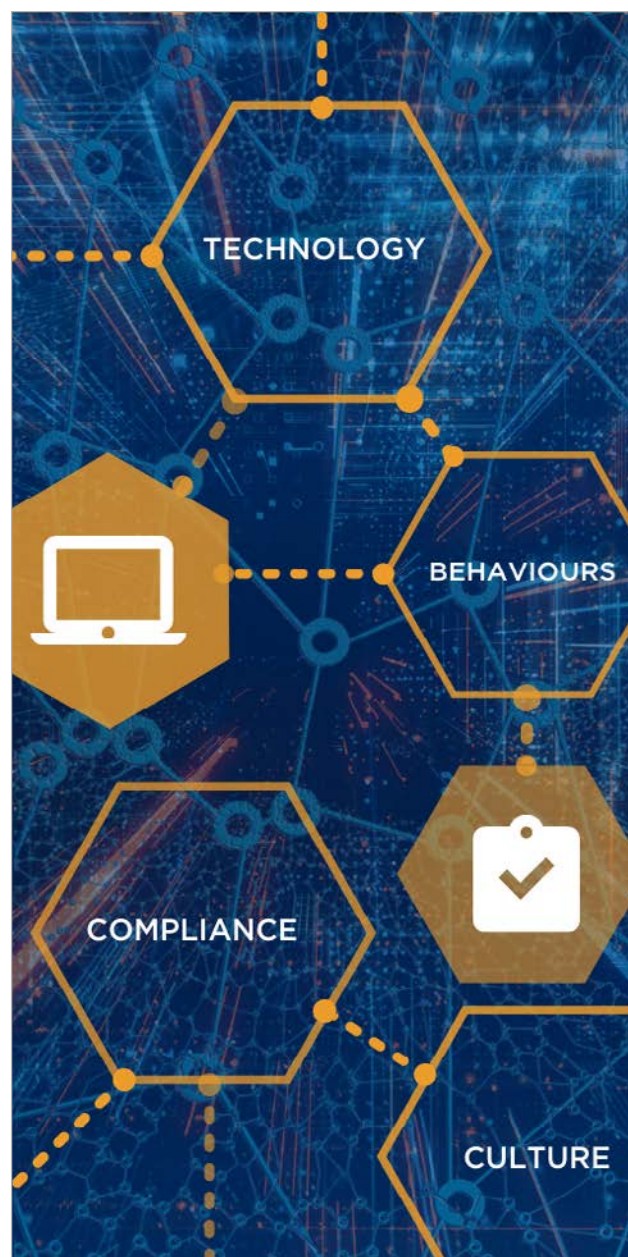
- **Failure to heed early warnings** – This denotes the absence of an effective corporate risk and governance framework that would have spotted irregularities. It took the intervention of a whistleblower to bring the matter to light.
- **Lack of appropriate governance** – The complacency of auditors, who took senior executive reports as evidence, without appropriate checks, led to continuous failings.
- **Failure to take regulatory compliance seriously and to spot accounting irregularities and internal fraud** – **McKinsey warned Wirecard’s Board a year before** of ‘significant risk’ and advised ‘substantial change’ in risk and compliance management. Wirecard decided to hire PWC instead, creating a potential conflict of interest as PWC were also the auditors for Wirecard Bank. →

- **Supply chain impact, leading to operational and reputational risk, as well as societal impact** – Wirecard’s failure resulted in a significant impact on their B2B customers, largely fintech firms, the more able of which had already been preparing to **distance themselves**. But consumers were still directly affected, denting trust in digital payment services.
- **Lack of Board commitment and accountability** – Whatever the Wirecard Board’s objectives were, it is clear that executive management were not leading by example. As bad behaviour was rewarded (or at least overlooked), and corners were cut, a toxic corporate culture took hold.

Getting results

Now more than ever, rather than relax risk postures, businesses must continue to apply (or step up) the rigour and governance needed to manage risks associated not only with supply chains but also with employees.

The increasing technological and regulatory complexity, as well as the increase in cybercrime and fraud, suggests the need for some form of technology automation, as I suggested in my **earlier post**, but any amount of technology, in and of itself, will not solve these challenges. Nor will regulations on their own, as they only provide ‘responsible’ operating frameworks. A combination of technology, regulatory compliance, culture, and behaviours are the key success factors for risk management to be effective. Losing sight of this can only lead to failure.



About EPA: The EPA is a thriving community of payments professionals aiming to strengthen and expand the payments industry. Since 2004, they have been instrumental in helping to connect the ecosystem, encourage innovation and profitable business growth. Over 130 member companies benefit from a comprehensive programme of activities, which addresses key issues impacting the industry.

www.emergingpayments.org



Challenges in Ecommerce

For a successful business, ecommerce merchants need to overcome some key challenges: balancing an excellent customer experience with frictionless authentication, reducing the time for processing orders or having the best fraud controls. Besides these, they face highly sophisticated fraud attacks such as merchant fraud, account takeover, chargebacks, no-transaction fraud or marketplace fraud. In this chapter, we have looked into the most impactful fraudulent issues that translate into ecommerce losses.

ACI Worldwide

Managing Fraud Successfully When Navigating the Digital Shift



About Fabian Gloerfeld: Fabian Gloerfeld is leading ACI Fraud Management since 2019 and is responsible to equip our customers with cutting-edge fraud and financial crime prevention solutions. Fabian is passionate about helping banks, merchants, and intermediaries to improve their bottom line by catching the ‘bad guys’ while allowing frictionless processing for genuine parties in a real-time enabled world. Prior to his current role, Fabian was leading ACI’s Strategic Programs Office of the Product Development organisation.

Fabian Gloerfeld ■ VP Fraud Management ■ ACI Worldwide

2020 has seen a rapid and unstoppable shift to ecommerce, but with this has come increased exposure to fraud. Fabian Gloerfeld, Head of Fraud Management at ACI Worldwide, offers his advice to merchants on how to navigate these challenges.

This year we have seen an extraordinary acceleration towards ecommerce and digital payments. What has been the impact on fraud trends and how is this affecting merchants?

When payment habits change, fraud habits change too. Across ACI’s global merchant customer base we’ve seen fraud attempts increase by 4% in the first half of 2020 and the average transaction value of attempted fraud is up 13%. This is despite the average value of genuine transactions decreasing during the same period. Without the right fraud prevention strategy during this period, a chargeback increase is inevitable.

“ Given the pace of change, merchants need agility in their fraud strategy and a flexible, sophisticated solution in place.

With unexpected peaks in transaction volumes and merchants busier than ever responding to customer demand, the instinct for many is often to tighten controls to prevent fraud and keep chargeback rates in check. Of course, it’s vital to protect your business from

fraud, but the wrong approach to fraud prevention can potentially mean merchants lose more money to the fear of fraud than to fraud itself. An overly strict approach to fraud prevention can introduce unnecessary friction to the payment process and result in false positives – both of which can damage customer relationships and cost merchants heavily in lost sales.

What advice can you offer merchants who are experiencing either an increase in fraud or an increase in declines alongside their increased transaction volumes?

Identifying genuine transactions and minimising false positives is as important as detecting suspicious anomalies and fraudulent transactions. Merchants need to examine their overall fraud Key Performance Metrics alongside their conversion rates and acceptance levels. The right fraud strategy must create a balance between all these metrics to optimise revenue, delight the customer, and yet successfully mitigate risks.

If merchants are not striking this balance, then the first thing they need to do is to understand why – analyse their transaction data (with skilled risk analysts), identify fraud trends and decline (as well as false positive rates) to figure out where the problem lies, and how they can address it.

You advocate that a holistic approach to fraud prevention can support increased sales as well as stopping fraud. Can you expand on this idea in more detail? →

Preventing fraud and minimising chargebacks is simply the bare minimum that a fraud prevention solution can achieve and quiet honestly, not the biggest challenge. The real aim should be converted in as much business as possible, but safely.

To give you an example, we recently were asked for help by a Tier 1 merchant whose chargeback rates were stable, but they were experiencing significant declines in acceptance rate (false positives – lost revenue) with their current fraud provider. Working with the merchant, we applied only our positive profiling in the transaction flow as part of the pre-authorisation screening. Positive profiling is one element of ACI's multi-layered approach and built on ACI's powerful data consortium. It helps us to identify genuine customers while ensuring a frictionless checkout experience. This process can also help anomalies stand out, so flagged transactions can undergo further scrutiny. In this case, the merchant was able to convert an additional USD 700k in revenue in the first month alone. The merchant's acceptance rate was improved by one percentage point. Additionally, we were able to reduce the number of Manual Order reviews that can increase the cost base for fraud prevention quite a bit. Decisioning should be automated where possible and manual reviews only executed as last resort. The cost of a manual check is between USD 1.5 and USD 3 depending on the provider. Imagine you could safely reduce these costs by 20-30%.

What additional fraud challenges do you see as causing hurdles for merchants as we go into 2021?

As Strong Customer Authentication (SCA) under PSD2 comes into effect in Europe, two-factor authentication – mostly in the form of 3-D Secure – will become more widely used, having the potential to cause sales disruption for many merchants.

To reduce the friction for as many genuine customers as possible, merchants should be working now to plan and agree their SCA exemptions strategy with their acquirer – as well as continuing to screen transactions for fraud themselves, to ensure that they hold down their fraud rates and, so, qualify for these exemptions.

Of course, consumer shopping habits will continue to evolve, with new buying behaviours, payment, and fulfilment methods. Merchants need to keep a watchful eye on the knock-on effects this will have on fraud and be prepared to adapt strategies to address emerging threats.

What tools and strategies do merchants need to have in place to be prepared for these evolving challenges?

A multi-layered solution, consisting of different mechanisms like machine learning, positive profiling, smart use of third-party intelligence via an orchestration engine to name a few, will give merchants the best chance of striking the right balance between fraud prevention and maximising the revenue intake from genuine customers.

Given the pace of change, merchants need agility in their fraud strategy and a flexible, sophisticated solution in place. Regularly reviewing fraud prevention strategies with external fraud experts will become more valuable than ever. Through the year end and into next year, customer and fraud trends will undoubtedly stay in constant flux, and failing to understand and adapt to these changing trends can be costly.

Learn more about ACI Fraud Management for Merchants [here](#).

About ACI Worldwide: ACI, the Universal Payments (UP) company, is a leading global provider of real-time, any-to-any electronic payment and banking solutions. Through our comprehensive suite of software solutions, delivered on customers' premises or through ACI's private cloud, we provide real-time, immediate payments capabilities, and we enable the industry's most complete omnichannel payments experience.

www.aciworldwide.com

[Click here for the company profile](#)

Arkose Labs

Understanding True Intent: Probabilistic vs Deterministic Approaches



About Kevin Gosschalk: Kevin Gosschalk formed Arkose Labs to build a revolutionary way to catch fraudsters online by focusing on their underlying objective – financial return. Arkose Labs' goal is to make it more costly to commit fraud and abuse than the potential reward, thereby removing the financial incentive and creating a world where all online identities can be trusted.

Kevin Gosschalk ■ CEO and Founder ■ Arkose Labs

For ecommerce companies, 2020 could be characterised as the best of times and the worst of times. Digital businesses saw massive waves of new customers as COVID-19-related lockdowns spurred people online to buy everything from cars to groceries to video games. And those who previously engaged in online commerce only occasionally, quickly became much more reliant on it.

This massive increase in traffic and customers was a boon for digital commerce companies, but like moths to a flame, it attracted more fraudsters than ever before. Fraudsters sought to blend in with this increased traffic, and commit attacks against companies and their customers before – or without – ever getting caught. With more people online than ever before, this meant that old fraud models of what constituted suspicious behaviour were thrown out the window.

At the same time, ecommerce firms are expected to deliver a seamless experience to consumers with no friction. Doing so while effectively fighting fraud presents quite the conundrum. The key is to combine a risk-based probabilistic approach that identifies potential suspicious behaviour with a deterministic approach that tests higher-risk traffic, and interacts with users to prove definitively their intent.

Who are you?

In this post-breach world, digital identifiers cannot be trusted or taken at face value. That's because years of massive data breaches have exposed nearly everybody's emails, passwords, and other pertinent data. All of this is in the hands of fraudsters, who carry out credential stuffing attacks at scale to take over good user accounts and commit downstream fraud.

Even more difficult to detect are synthetic identities, which use a combination of real consumer data and fictitious information. Attackers will use an array of tools to obfuscate and spoof digital identifiers to evade traditional fraud detection models.

This problem is exacerbated in a year which has had an influx of 'digital debutants' as lockdowns have forced new sections of society online. Risk models that rely on previous behavioural norms are a far less reliable indicator of trust.

Many businesses rely on risk scores to help identify bad traffic, but these can tell you a certain user might look suspicious, but not what to do with it. Do you get overly conservative, and block any traffic that might seem suspicious and risk alienating potential customers that fall into this net? Taking the opposite approach, and letting in all but the most obviously bad traffic, opens up your platform to fraud attacks which not only drain revenues but harm the experience for your real customers as well.

In order to make sense of these risk scores, in a world where increasing amounts of traffic falls in the 'suspicious' bucket, it takes a lot of manual reviews from internal fraud and security teams. This creates inefficiencies and overly burdens internal teams, who could be spending their time doing more value-added tasks rather than manual fraud reviews. It also hurts the customer experience, as users have to wait a while before being authenticated and allowed onto the platform.

Another approach that has proved problematic is relying on out of band authentication such as two-factor authentication. Consumers shop online because it is a quick and easy experience. →

2FA adds a great deal of friction to the authentication experience – most consumers hate it. Things like SMS tokens also punish people who have bad cell phone reception at the time, for example, or use VOIP. Fraudsters on the other hand can easily set up fake accounts to bypass SMS or physical tokens.

How to determine true intent

Businesses need risk-based insights that provide a clear path to real-time remediation, without forcing users out of band and killing conversion rates.

Optimal fraud and abuse detection should classify traffic based on suspected intent and then test and interact with the traffic for a more deterministic approach. The first part involves robust detection capabilities. This should include analysing hundreds of data points and utilising behavioural biometrics such as real-time data around device and fingerprint ID as well as behavioural data. This is important since bad actors will generally behave differently because of the monetary incentives. This includes filling out forms quicker, copying, and pasting data, and generally working much more quickly than real customers in order to complete tasks at scale.

After that, traffic can be accurately segmented into bots, good users, and potentially suspicious users. Many actual customers may fall under the latter category for a variety of reasons. That's where user-friendly secondary screening comes in. It should be something that is designed to be nigh-on impossible for bots to solve and frustrates fraudsters carrying out multiple attacks, but very easy for good users. With accurate detection classification, most good users shouldn't need secondary screening at all, but for

those who do, it should be easy to pass through and be much less antagonistic than traditional MFA.

Testing the responses of traffic posing as a legitimate consumer can happen in several forms – behind the scenes or through in-session user challenges. The trick is to combine risk insights with secondary screening in order to obtain more evidence of true intent. This avoids relying on a purely probabilistic approach, or forcing users out of band and slowing transactions down.

This way, ecommerce firms can keep good customers happy, while frustrating the bad guys, to the point that they abandon attacks.

About Arkose Labs: Arkose Labs bankrupts the business model of fraud. Recognised by Gartner as a 2020 Cool Vendor, its innovative approach determines true user intent and remediates attacks in real time. Risk assessments combined with interactive authentication challenges undermine the ROI behind attacks, providing long-term protection while improving good customer throughput.

www.arkoselabs.com

[Click here for the company profile](#)

SecuredTouch

The Growing Popularity of No-Transaction Fraud



About Alasdair Rambaud: Alasdair is a seasoned C-level general manager with 20+ years experience managing large global organisations with a focus on Sales and Strategy. He holds a Masters in Business Economics from Reims University, France.

Alasdair Rambaud ■ CEO ■ SecuredTouch

The Paypers sat down with Alasdair Rambaud, CEO of SecuredTouch, to discuss the growing threat of no-transaction fraud, the challenges in detecting it, and how using behavioral biometrics prevents it.

What is no-transaction fraud and why is it challenging to detect?

As opposed to payment fraud, which occurs at the checkout stage, with the fraudster actually performing a transaction on the merchant's website or app, no-transaction fraud happens earlier in the buyer's journey. Although no-transaction fraud doesn't result in a direct purchase via the checkout process, it can cause substantial damage to the business.

“Understanding the fraudster's journey is vital for identifying no-transaction fraud without compromising the legitimate buyers' experience.”

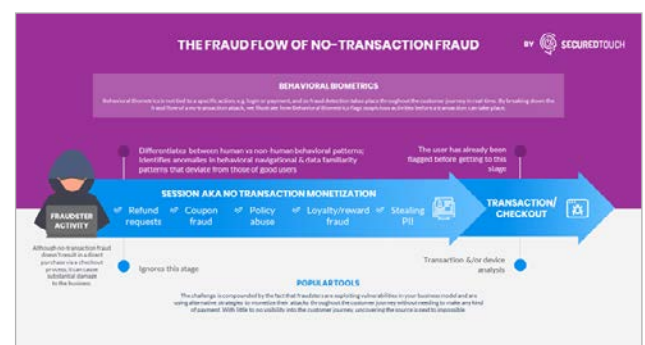
Examples for such fraudulent activities include refund requests, for goods not actually purchased; coupon fraud, where coupon codes are maliciously obtained; and **loyalty and reward fraud**, where points are redeemed against goods or services or are sold to others. In addition, fraudsters have much to gain from stealing personal identifiable information (PII), which can result in identity theft and stealing credentials to use in other websites/apps or sell to other malicious actors.

As we can see, the fraudulent activity is not a transaction, but a variety of possible fraudulent actions, which all happen early in the buyer's journey, and where traditional fraud detection tools have little to no visibility of activities taken by legitimate or malicious users.

Also, implementing rule-based fraud detection to cover the entire buyer's journey, will inevitably lead to a high number of false positives and end up frustrating legitimate customers. When these are the options, merchants tend to choose happy customers and a troubling fraud rate over losing customers and catching fraudsters.

What makes these fraud methods attractive to fraudsters and how do they evade fraud prevention tools?

Payment fraud tends to be picked up by popular fraud detection tools, which is why fraudsters found new ways to carry out fraud and avoid being detected, earlier in the buyers' journey. They found a significant gap in the solutions that allowed them to exploit the business model. →



Infographic: Fraudsters have found ways to monetise earlier in the customer journey without the need to make a traditional transaction thereby avoiding the need to beat transaction or device analysis tools.

Yet, online merchants are reluctant to add fraud prevention tools earlier in the buyer's journey, as they are concerned about the friction it will add to their legitimate buyers' experience. This leaves plenty of opportunities for malicious actors to carry out no-transaction fraud.

Retailers are rightfully concerned with the need to ensure that detection of fraud early in the process (early enough as to prevent damage, including chargebacks) will introduce as little friction as possible into the customer's journey.

'Sometimes it seems that retailers can't win'

Sometimes it seems that retailers just can't win: If they flag an activity as suspicious based on strict rules, they might find themselves with a rise in false positives and possibly disappointed legitimate customers. Other times, retailers rely solely on fraud detection and prevention at the payment stage, ignoring any potentially suspicious activities that occur earlier in the customer journey. The magnitude of no-transaction fraud is growing fast, as fraudsters are continually developing advanced evasive techniques and increasingly using automated tools, such as bots and emulators, to scale their attacks.

What sets behavioural biometrics apart from other approaches in preventing no-transaction fraud?

Adopting advanced technologies like behavioural biometrics enables us to take a proactive approach to preventing fraud, by providing complete visibility into fraudster's activities throughout the entire buyer's journey. In-depth understanding of the fraud journey, identifying, monitoring, and analysing data from various touchpoints, make it easy to detect suspicious and potentially fraudulent behaviour at its earliest stage.

The ability to automatically differentiate between human and non-human behaviour and to identify behavioural anomalies can clearly indicate fraudulent activities at an early stage, without the need to add friction to the buyer's journey.



How can merchants improve their business efficiency via solutions similar to the ones offered by SecuredTouch?

Detecting fraud early in the fraud journey is usually based on identifying fraudulent intent as opposed to fraudulent activities, which means before any damage has been done. To get there, merchants need to apply a holistic approach to their fraud prevention strategy. Solutions must be able to monitor user activities and behaviors from the moment a session begins and carry out continuous discovery, throughout the customer journey. The better we understand the journey of fraud, and the more accurate insights we have about human and non-human fraudulent behaviours, the easier it will be to differentiate between the actions of good users vs fraudsters.

SecuredTouch applies behavioural biometrics to continuously analyse human-to-device interactions throughout a session, to accurately validate trusted users and the device legitimacy. This approach enables merchants to stop fraudsters long before the transaction stage, reducing fraud while maintaining the balance between customer satisfaction and security.

About SecuredTouch: SecuredTouch provides real-time, adaptive fraud detection throughout the customer journey to detect fraud early, with proven ROI from day 1. Our solution ensures accurate risk-based prevention for multiple use cases including ATO, bots, and no-transaction fraud. SecuredTouch customers benefit from reduced overall fraud losses while maintaining a smooth customer experience.

www.securedtouch.com

[Click here for the company profile](#)

About-Fraud

Merchants Need to Be a Mastermind in Today's Ecommerce World



About Ronald Praetsch: Ronald is Co-Founder at About-Fraud and consults regularly with merchants, payment service providers, and fraud solution vendors. Before About-Fraud.com, he spent close to a decade in various payments and fraud prevention roles.

Ronald Praetsch ■ Co-Founder ■ About-Fraud

Merchants are facing many challenges in 2020, which are stretching the mind in different directions. Many ecommerce merchants are overwhelmed with the current situation and many topics link to one another.

The COVID-19 situation has hit many ecommerce merchants hard without any preparations. Today, in the US and Europe, many traditional retailers are still heavily relying on retail stores. From one day to the next, stores were closing, and the main revenue channel got shut down.

This situation forced retailers to the ecommerce channel and not everybody was ready for this change. Today we see many retailers without a dedicated ecommerce team who is looking at the checkout experience, payment topics, and fraud prevention. Now, you can imagine the challenge for these companies to become an online first organisation.

We have seen a range of fraud topics which ecommerce companies are facing right now:

Accelerated refund fraud

Refund fraud is not new but it gets more professional and therefore more accessible for a broader audience. Today, professional refunders are offering their services via specific social media channels where they provide step by step instructions. Once the customer received the item, the professional refunder will provide the full documentation which is needed for the refund. The professional refunder knows the process and guideline from the relevant merchants for refunds. Therefore, the customer will pay, for a successful refund, a commission to the professional refunder.

Refund fraud comes in several types and fraudsters become very creative:

- did not receive item;
- empty box arrived;
- partially delivered;
- return empty box.

The advice would be to:

- start to capture all relevant data about your refunds;
- remember, often refund information is not captured or not connected to your payment and fraud data;
- include your customer service information with your fraud review.

Social engineering

This is impacting customers and merchants in different dimensions and, without the right data and tools, it is not easy to detect. Phishing attacks are an increasing fraud trend, especially spear phishing emails, and this is revealed in statistics provided by industry reports such as [APWG's Phishing Activity Trends Report](#) and Symantec's Internet Security Threat Report. As well, according to Kaspersky's [spam and phishing report for the second quarter](#), the overall number of phishing attacks in the quarter reached nearly 130 million.

The goal of the phishing attacks is to get access to customer accounts or capturing customer data that are used by the fraudster to purchase items at the ecommerce retailer. The inexperienced ecommerce retailer will not see a difference between a normal account and a compromised one. Many retailers might use a legacy white list which will offset many fraud rules. →

The advice here is to:

- capture data about your account creation, account login, and account changes;
- don't use stand-alone white list rules which can be easily used to exploit your fraud solution;
- stay up to date about new trends in the industry to review your processes, policies, and tools.

PSD2-SCA is not over

With the upcoming enforcement data for many countries in Europe (1 January 2021), there are still some merchants that have showed limited knowledge about PSD2, and some are not fully paying attention to the real business impact of this topic. PSD2 and the related SCA requirements have been on the radar for a long time but deadline postponements, new local regulator plans (such as the introduction of soft declines) are pressing the nerve of the merchants and the ecosystem.

Right now, all merchants need to make sure that PSD2-SCA is correctly implemented. We see the most important aspects in:

- requesting 3DS authentication according to the merchant use cases;
- ensuring the right data are sent to increase the possibilities of Issuers Risk-Based Authentication;
- monitoring performances and have a 2021 PSD2 strategy (exemptions, 3DS 2.2, delegated authentication etc.).

On one side, merchants are heavily dependent on their payment providers and how these PSPs implemented different acquirers. Many parties do support only basic features related to 3DS2 but are not leveraging the full potential of PSD2 to reduce customer friction.

The advice here is to:

- have a dedicated person managing PSD2-SCA in all aspects;
- implementation, update from the schemes and regulator, payment provider communication and data review.

Payment provider melting down

In the summer of 2020, Wirecard filed for insolvency and many merchants realised a massive dependency on one payment provider. Not every merchant has the luxury to run a multi-payment provider setup to mitigate such risk. Besides this situation, a multi-payment provider setup can provide you leverage for better authorisation rate and a better situation when it comes to negotiating your contracts.

The advice here is to:

- review your current payment provider setup and understand the dependencies which you are facing;
- build or buy discussion on how to connect to multiple payment providers: using a payment hub or building your own.

Overall, in Q4 2020 ecommerce merchants have a long list of topics to deal with and in 2021 they will face further challenges.

About the company: About-Fraud is a Global Community for fraud fighters. Our community was born from an industry need for unbiased, educational fraud prevention resources. About-Fraud filled that gap with a platform that connects fraud fighters with the information they need to understand the technology and trends, grow their career, and stop fraud.

www.about-fraud.com

Breach Clarity

How the Pandemic Will Feed an Account Takeover Explosion



About AI Pascual: AI is the COO and Co-Founder of Breach Clarity. A recognised expert in financial crime, AI's insights on the effects of fraud have been published by hundreds of publications and shared with attendees at industry events around the world.

AI Pascual ■ COO and Co-Founder ■ Breach Clarity

Calamities breed fear, which in turn creates opportunities for fraud. And it is becoming painfully clear that this pandemic is a boon of epic proportions for fraudsters everywhere. Between COVID-19 scams targeting consumers, the wholesale theft of government benefits, and playing on the financial worries of the newly unemployed, 2020 will undoubtedly go down as one of the costliest on record when it comes to identity crimes. As for merchants, they are far from unscathed, but the challenges they face are unique – not only in how they manifest but as to why they are occurring and are likely to get worse. Four factors, some newly emergent and others long unaddressed, are coalescing to overwhelm an already beleaguered industry. Unfortunately, pressure from fraudsters will only become more intense, and for many merchants, survival will require finding a way to disrupt these factors before it is too late.

For merchants struggling with the implications of massively depressed sales activity, increasing online transaction volume is far from a panacea. Those merchants that are fortunate enough to continue their sales operations online are finding that the mass migration of shopping activity to digital channels is exposing them to increased risk. This dynamic has played out time and time again – whenever there is more transaction volume of any kind, fraudsters will follow. And according to LexisNexis, the pandemic has only made matters worse as the rate of fraud attempts has increased even more dramatically since the economic slowdown began.

Ironically, the continuing rise of ecommerce fraud will be inextricably tied to how the fall of point-of-sale traffic is affecting the use and availability of compromised data:

When it comes to using compromised data to commit fraud, fraudsters are avoiding physical storefronts just like the rest of us. Even with a solid supply of point-of-sale card data from older breaches available on criminal forums, fraudsters are not willing to risk their own health and increase the chances of getting caught red-handed at nearly empty merchant locations. This is clearly demonstrated by the fact that the going price for compromised point-of-sale card data is down, but online card data is still selling for a premium on criminal forums.

Without legitimate sales activity at brick-and-mortar locations, the available pool of compromised card data is beginning to dry up. Over time, this will drive a further shift of fraudulent activity from the point-of-sale as fraudsters look for alternative data sources to support other types of crime. According to Breach Clarity's own data, the proportion of new breaches capable of fueling card fraud is much lower than only a few months ago, but those contributing to the risk of account takeover (ATO) are relatively undiminished.

The risk of card fraud is falling off a cliff as card breaches become fewer and farther between

Figure: Percentage of fraud risks created by newly discovered data breaches, by month →

The most serious pending threat to merchants lies in this unchanging frequency of data breaches capable of fueling ATO. Account takeover using compromised credentials obviates the need for fraudsters to have access to stolen card data, as saved payment information can be easily misused once they have access to a victim's existing account with a merchant. And retailers are the most heavily targeted industry segment for credential stuffing attacks that can lead to ATO, **according to a 2019 report from Akamai**. This makes sense when you consider that organisations like financial institutions often deploy far stronger forms of authentication than the typical merchant. So, until strong authentication becomes more the norm than the exception, fraudsters armed with compromised credentials will only drive ATO higher among ecommerce merchants.

It is an old and oft-used adage that 'criminals go where the money is', but it is just as true now in the case of ecommerce fraud as it has ever been. The changing channel preferences of consumers – an acceleration of the shift from the point-of-sale to ecommerce due to COVID-19 – is driving where fraudsters can and will focus. Armed with stolen card data today, and with an increasing reliance on compromised login credentials (and other data that can support ATO attempts), the risk that fraudsters pose to ecommerce merchants has never been more certain, or more serious. Ecommerce merchants can little afford to suffer increased fraud losses. This is especially true for those with legacy brick-and-mortar locations that are being ravaged by mandatory shutdowns, or at a minimum massively reduced foot traffic. Criminals are opportunistic and will often avoid the hard targets for the easy mark. For the foreseeable future, the 'marks' are those ill-equipped merchants that will suffer just when they can least afford to.

About Breach Clarity: Breach Clarity is a fraud prevention and detection technology firm based in the San Francisco Bay Area. The company's AI-based technology provides consumers and financial institutions with clear analysis and guidance around data breach-related fraud and identity risks.

www.breachclarity.com

Dunkin' Brands

Tackling Fraud Challenges in Ecommerce



About Patrick Finnigan: Patrick Finnigan is the Director of Loss Prevention Analytics and Fraud at Dunkin' Brands. Supporting two iconic brands, Patrick leads the Loss Prevention Analytics, Digital Fraud Prevention, and Corporate Fraud functions in support of over 21,000 locations in over 60 countries. Prior to his role with Dunkin' Brands, Patrick was a Medicare Fraud Investigator and has a combined 20 years of experience in fraud, loss prevention, and data analytics. Patrick is known for developing innovative and measurable programmes and initiatives that support franchisee and brand profitability through the integration of fraud tools & technologies, data analytics, and a holistic approach to fraud prevention.

Patrick Finnigan ■ *Director of Loss Prevention Analytics and Fraud* ■ Dunkin' Brands

With the surge of online and mobile purchases, fraudsters have also seized the opportunity to explore any vulnerability or loophole in the ecommerce space, causing merchants to wisely rethink their strategies so they can ensure a secure and convenient customer experience. At the same time, solution providers are pushed to further innovate their services and technologies to keep fraudsters at bay and help their merchants boost their revenue and protect profits. In a high growth environment like the ecommerce space, several particular challenges remain top of mind so that businesses can increase revenue, expand digital enablement, and drive customer loyalty.

Omnichannel success depends upon a multi-layered fraud mitigation strategy

While some businesses had already offered a variety of channels for customers to interact and engage with them, the onset of the pandemic in early 2020 forced many merchants to accelerate their omnichannel and digital plans. While this opened up new streams of revenue, it also produced a host of new and previously unseen points of fraud exposure that merchants needed to protect against. As such, it is increasingly clear that merchants need to guard against fraud along the entire customer journey – not just at the time of financial transaction. This means putting protective measures in place at account creation, login, add a credit card, loyalty programme sign-up etc. Those newer to omnichannel and digital commerce struggle with these types of issues as they

have not planned for and invested in fraud solutions designed specifically for the risks associated with the mobile channel and digital transactions. As merchants come to understand that it is imperative to open these channels in order to generate revenue in the current landscape, they should understand the importance of protecting profits with a multi-layered fraud mitigation strategy. Successful digital transformation requires balancing three critical areas: user experience, fraud mitigation, and revenue generation or business goals. The extent to which IT/cybersecurity, fraud teams, and digital/mobile teams are integrated and talking to each other is critical to an organisation's ability to fight fraud, protect the digital customer journey, and protect revenue. A layered approach to fraud mitigation protects profits, your customer's data, and the reputation of your brands.

Gift cards are very appealing to both consumers and fraudsters alike

Gift cards are an attractive target for fraudsters for a variety of reasons. First off, they are very easily monetised. Gift cards can be bought and sold on many third-party websites, in both digital and physical form, making it very easy for fraudsters to monetise their ill-gotten gains. Digital gift cards, in particular, can be easily obtained by fraudsters who purchase them using stolen credit cards. This is probably the most widespread form of gift card fraud. →

The cards are hard to trace and are not subject to the same scrutiny as debit or credit cards, therefore making them attractive to potential buyers. Fraudsters can also tamper with physical gift cards on display at the point-of-sale by merchants by either copying gift card numbers, bar codes, or QR codes, and then waiting for the cards to be activated by legitimate buyers. Once activated, the fraudster can drain the balance of the card in CNP transactions online. Merchants that sell gift cards via mobile, web, and point-of-sale need to ensure appropriate safeguards are in place to protect both consumers and merchants alike.

Fraud detection in real time may be difficult with sparse or unlabelled data

Device data collection via an SDK is critical to assisting with fraud mitigation. Collecting device data in real time that can be used to analyse characteristics of the persona conducting the transaction is very important when there is little data input to analyse, as is the case in guest checkout type transactions for instance. Collecting and analysing data points and information gleaned at the time of transaction will enable your fraud tool to make better decisions based upon information related to the device, user, and transaction. For instance, if you can tell that a device is 2000 miles away from the credit card billing address, you may subject the transaction to a different level of scrutiny. Machine learning, AI capabilities, and large amounts of consortium data from other merchants are also helpful when the transactions themselves have little or unlabelled data.

Choosing the right fraud prevention solution provider

Choosing a fraud solution provider can be a daunting task. There are many criteria to consider when vetting fraud management vendors and it is important to first understand exactly what your own business needs are before looking at potential solutions. Of the many important criteria to consider, some stand out more than others. Cost is, of course, top of mind for all, as you need a solution that makes sense from an ROI perspective. You also will want a tool that can detect a wide range of fraud through a combination of machine learning, AI, and an advanced rule engine. The system should not solely rely on rules, as fraud attacks are increasingly more complex and sophisticated. Ease, time, and cost of integration is also a factor to consider, as this may impact your ability to get the tool up and running effectively. Flexibility or ability to work with multiple channels (mobile/web etc.) is also a critical component. Finally, you must be sure to leverage references from merchants both within your vertical as well as from other sectors, as they can provide you with valuable information regarding the tool's capabilities, shortcomings, and other lessons learned from integration to day-to-day performance.

About Dunkin' Brands: With more than 21,000 points of distribution in more than 60 countries, Dunkin' Brands is one of the world's leading franchisors of quick service restaurants (QSRs) serving hot and cold coffee and baked goods, as well as hard serve ice cream. Dunkin' Brands is the parent company of two of the world's most recognised and beloved brands: Dunkin', America's favourite all-day, everyday stop for coffee and baked goods, and Baskin-Robbins, the world's largest chain of ice cream specialty shops.

www.dunkinbrands.com

Ecommerce Foundation – Scamadviser

Fighting Online Merchant Fraud Must Be Done Globally and Is Essential to Keep Trust in Online Payment



About Jorij Abraham: Jorij Abraham has been part of the international ecommerce community since 1997. He has been ecommerce manager at Bijenkorf, TUI, online publisher at Sanoma Media, and Director of Consulting as 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.

Jorij Abraham ■ *Managing Director* ■ Ecommerce Foundation – Scamadviser

In our industry we tend to focus on two kinds of online fraud: consumer fraud, where the consumer is misusing credit card details and other payment methods, and money laundering, where criminals use payment services to conceal the origins of illegally obtained money. There is however a third kind of deceit which deserves at least the same level of attention: online merchant scams.

Online Merchant Fraud means criminal activities where consumers lose money, confidential data or other assets via a deceptive online act. There are many types of online scams from online shopping (products not being delivered), fake products being sold, cryptocurrency trading (men have a tendency to fall for these), investment plots promising 1% daily returns (popular in low income countries like India and Indonesia), Ponzi and pyramid schemes (mainly targeted at elderly), subscription scams (generation X & Y), romantic dating scams (victims are mainly middle-aged women).

While being a scammer is probably the second oldest profession, since the start of the coronavirus crisis there has been seen a traffic increase with **40% on Scamadviser.com**. Firstly, mainly around masks and hand sanitisers which were not delivered. Currently, there is a general rise around all kinds of scams.

Scamming has become Big Business

Online fraud has been increasing for years as the graph below shows. Scamadviser's sources state that several crime networks are moving away from human trafficking and narcotics towards online scams, as they have a low risk of getting caught, require few upfront investments, and are extremely profitable.

Figure 1: Billion Lost and Number of Complaints in the USA.

Source: FBI Crime Complaint Center, 2019

The second reason why the number of scams is exploding is that, with COVID-19, some crimes have become more difficult to execute, as border controls are enforced more strictly.

In the last few months, Scamadviser has been confronted with several networks which specialise in one kind of dubious practice.

These networks are increasingly meeting global ecommerce standards, offering multilingual websites, 24-hour pre-sales chat support and a wide range of payment methods. They not only use social media to gain traffic but also use paid advertising, especially on Facebook and Google. They can easily afford the advertising fees as their profit margin is nearly 100%.

They do not operate in their own country and keep the number of chargebacks and complaints per registered company low to stall the moment of being banned by Visa, Mastercard, PayPal, or the payment service provider. After being banned on one website, traffic is redirected to the next website and registered company and the game starts anew. →

Online scams are hurting online trade & payment

The sharp rise in online merchant fraud is starting to affect the ecommerce industry. Consumers are becoming hesitant to buy online or are falling back to '100% safe' sites such as marketplaces. This trend is not only hurting smaller online initiatives and start-ups which yet must build up consumer trust. It is also harming whole countries. The number of scam sites from China has reached such high levels that many western consumers are becoming hesitant to order anything from an Asian looking website. Likewise, Chinese consumers looking for exclusive brands are hesitant ordering from a '.ch' (the Swiss domain extension) site, fearing it may be fake.

The growth of online scams is hurting the payment industry. Professional scammers have proven capable of setting up a company in bulk. Once identified as a scam, they simply hop to the next payment service provider or 'just in time' founded company. Only fingerprinting of the site itself allows fast identification of an online scammer.

Central registration is a must

In the last few months, Scamadviser.com has worked on an ad-hoc basis with Europol and other parties to identify corona scammers. In the Netherlands, online scams can be reported to at least 7 different entities, who, due to the GDPR regulations, are often not allowed to share data. In other European countries online scam registration is often very decentralised (up to local police stations) or not organised at all.

Each payment method and PSP is maintaining its own 'black list' of scammy merchants, allowing criminal networks to keep hopping from service provider to service provider.

Taking into consideration that **only 3 to 5% of the consumers who get scammed online actually report the scam** to at least one authority and the fact that professional scammers distribute their activities across the globe, scamming is becoming a very attractive and 'safe' business.

Central registration of online scams, at least on a European level, but preferably global would be required to quickly identify online criminal networks. Combining reports from national police forces, consumer authorities, with complaints received by payment providers and feedback on review sites and social media allows quick identification of websites causing harm.

Scam reports can be linked together using fingerprint technology to identify scammers utilising the same scam across multiple websites. Clustering scam reports not only allows police forces to focus their enforcement activities, it also prevents double work across countries. In short, there is work to be done by entities such as Europol and Interpol to make the Internet a safer place to buy.

About Ecommerce Foundation – Scamadviser: The mission of the Ecommerce Foundation is to foster global digital trade. The company realises its goals amongst others with Scamadviser.com. Scamadviser is an online algorithm to identify online stores not delivering goods, shops selling fake products or sites offering high risk or illegal products and services.

www.scamadviser.com

Mango

We dig into known and emerging fraud trends in retail with Carlos Madrona Guillén, Internal Control & Compliance, Payment Methods and Fraud Director at Mango.



About Carlos Madrona Guillén: Carlos Madrona, with a huge experience in payment methods and fraud management, joined the company in 2015 as Head of Online Fraud. In July 2017, he was promoted as Director of Payment Methods and Fraud, a position in which among others he aims to lead the strategy of payments and fraud, online and offline in all the markets where Mango has presence. Recently, he has acquired a new role leading the Internal Control and Compliance team.

Carlos Madrona Guillén ■ Internal Control & Compliance, Payment Methods and Fraud Director ■ Mango

With Buy Online Pick up In Store (BOPIS), as well as Buy Online, Pick up at the Curb (BOPAC), or BORIS surging amid COVID-19, have fraud types such as BOPIS fraud, refund fraud also increased?

It is true that with this COVID-19, online orders, in general, have skyrocketed incredibly, and this has had a positive effect for the business, but on the other hand, it has represented a very hard time in the containment of fraud. Unfortunately, the stores have closed for a while, so that any fraudulent customer relationship with the stores has been minimised. However, in the face of the avalanche of online sales, the fraudulent customers have completely changed their approach and their performance, which has allowed it to blend in very well with legitimate customers.

“The most important thing is not the data the clients leave, but how they behave. Information is power.”

That has meant an incredible job for the fraud team in separating the big wheat from the chaff and being able to analyse behaviours, create new patterns of legitimate customers and fraudulent customers that have allowed us to detect them and therefore stop that fraud.

Once customers return to buy in stores regularly, these services will have special relevance, basically because they are strategic for businesses that seek to provide an omnichannel experience.

What about the old patterns such as ATO, omnichannel fraud? Have fraudsters improved their tactics and took advantage of the loopholes even more?

One thing we've been working on for a long time is studying customer behaviours. I think it is very relevant not only to focus on how the customers behave in the trade itself, but what they do outside, anonymously of course. This strategy enriches the information and facilitates decision-making, as your client behaves outside your company with a high degree of probability that they will behave the same in yours.

This is critical in fraud, because yes, the business always goes after the fraudulent, but if you know how the fraudster behaves both outside and inside, you can establish rules that allow you to have alerts, not deny directly, because companies are to sell and consequently make the best decision for your business.

Obviously, those who are dedicated to fraud know about this and what they do is increasingly resemble legitimate clients, therefore, if you only stay with what a client does within your business you are missing a part of the movie. And to see the full movie, machine learning tools, agile providers, and, above all, a great team constantly monitoring this data with the objective are key. →

What is the situation with chargebacks, especially in fashion retailing? More illegitimate chargebacks this year?

Unfortunately, during this crisis that we are experiencing, chargebacks have increased in many new businesses that due to the COVID-19 situation have been forced to run online stores.

Other large merchants that had the fraud team as a commodity have also been impacted by an increase in fraud that has led to a growth in chargebacks. In our particular case, due to all the efforts we make in the area of fraud and total alignment with the business, we have been able not only to detect fraud but also to stop it, reducing chargeback ratios and considerably increasing acceptance. The fraud team in our company not only has the mission of fraud prevention but also that of selling more, and now more than ever.

What best practices would you share for successfully handling large volumes of online sales in a frictionless and secure way?

There is no exact science to managing fraud, and every fraud manager has his or her own way. Mine is based on five premises:

- a) unless proven otherwise, all clients are legitimate;
- b) the devil is in the detail;
- c) the most important thing is not the data the clients leave, but how they behave – information is power;
- d) it is mandatory to know what business is expected from the fraud team;
- e) a recurrent customer is the one with a frictionless satisfactory shopping experience.

That being said, a company that can manage fraud effectively must make every effort to red-carpet legitimate customers and make life miserable for fraudulent ones.

What is your take regarding the life of ecommerce after SCA?

Honestly, nobody knows exactly what is going to happen. The regulations still have some incongruous points that PSPs/acquirers/issuers or even schemes don't know how to solve. On the other hand, the EBA says that it will meet the scheduled start dates today.

I think that with all this regulatory change, the trade has been blamed a lot and this has forced us to make extraordinary developments because we do not want our clients to be impacted. But who really should be prepared is each and every one of the European issuers and in turn, the PSPs and processors. It does not make sense for a business to be prepared if the one who has the last word is not. A lot has been thought about regulating but little about the customer experience.

Therefore, in order to prevent this looming chaos, we have raised any of the scenarios that can happen with this, and we hope to have a high volume of frictionless transactions.

I must also say that I expected more from the PSPs, not in terms of advice on PSD2, but rather I expected them to launch alternative products that would enhance Open Banking to provide a solid alternative to card payments. This has not happened yet.

Nevertheless, I think there will clearly be a 'before and after PSD2' I will tell you in our next interview.

About Mango: MANGO was founded in 1984 and is today one of the leading fashion groups in the world. Based in its city of origin, Barcelona, the company has an extensive network of more than 2.100 stores in 110 countries. From its 'El Hangar' Design Centre in Palau-solità i Plegamans, every year it designs more than 18,000 garments and accessories for wearing the season's trends. The company closed the 2019 financial year with sales of EUR 2.3 billion. More information at www.mango.com

www.mango.com

Marketplace Risk

Hidden Frauds That Translate Into Marketplace Losses



About Jeremy Gottschalk: Jeremy is an expert in risk management, trust & safety, and legal strategy for marketplace startups. With 15+ years of experience as a lawyer, operator, and consultant to insurance companies, investors, founders and operators, he has become an industry-leading voice. Jeremy founded Marketplace Risk as a platform for education, networking, and information sharing for the marketplace ecosystem. Jeremy holds a JD from Loyola and an MBA from Kellogg.

Jeremy Gottschalk ■ CEO ■ Marketplace Risk

McKinsey reported that US ecommerce penetration doubled during the early months of the COVID-19 pandemic, **which represents 10 years of growth**. The result is that one-third of all US business flows through ecommerce, **replacing physical channels**. Of all the ecommerce sales, **63% is transacted through marketplaces**. With so many more transactions, it follows that fraud has increased as well. According to **Arkose Labs**, the pandemic has brought on 'heightened attack rates, significant spikes in fraud attempts and greater volatility than in 2019', resulting in a **doubling of attacks over a six-month period**. In this article, we look at a few common types of fraud that have increased as a result of the pandemic.

There are many variables that explain the increase in marketplace fraud resulting from the pandemic. First, the increase in online transactions creates more opportunities for fraudsters, especially with lockdowns and quarantines causing consumers to work, shop, and bank remotely. Second, with incentives for fraudsters increasing, so, too, do the amounts and sophistication of fraudsters. Third, related to the second, the economic collapse in so many regions has caused widespread desperation, leading people to find 'creative' ways to make money. Fourth, many businesses have been forced to sell online in order to survive, but they have little-to-no understanding of the fraud landscape and are ill-prepared to combat fraud. Fifth, even marketplaces with experience fighting fraud are not prepared for the rapid growth in volume and their pre-pandemic fraud-fighting blueprints quickly have become antiquated.

Whether you are a legacy marketplace or bringing goods and services online for the first time, the fraud behaviour looks essentially the same, although the level of sophistication varies. And, with the urgency and immediacy driving spending habits during the pandemic, catching the fraud is complicated that much further. Therefore, consumers expect necessary and, in some cases, life-dependent goods and services right away (and often on a daily basis). This makes it difficult to identify and prevent fraud from happening at the speed and volume of the transactions. Here are a couple types of fraud that have proliferated during the pandemic.

Fake profiles

Marketplaces are driven by user-generated content. In fact, one of the hallmarks of marketplaces is the ability for buyers and sellers to transact through a passive intermediary without any substantive intervention. This often means that the platform does not verify the profile or the veracity of the information in the profile – the marketplace simply facilitates the transaction. As a result, it is quite easy for sellers to create fake accounts to sell bogus goods or services to unsuspecting buyers. In bad cases, sellers offer expensive goods (often at discounted prices) and buyers will be out significant sums. In the worst scenarios, sellers steal buyers' credit card information from transactions and, combined with buyers' personal information, can use credit cards for other nefarious purposes later. →

For the more sophisticated fraudsters, profiles will often mirror known, legitimate sellers, complete with fake reviews and testimonials to add credibility. Unknowing buyers purchase items at too-good-to-be-true prices, but never receive them. By the time buyers realise they have been scammed, so, too, have many other unwitting consumers and fraudsters vanish into thin air (not that they ever appeared in the first place).

Stolen credit card purchases

It's no secret that hacked financial and personal information is readily available on the dark web. But, fraudsters have many other avenues to access information beyond the dark web, including by collecting information from purchases through fake profiles or, with a little bit of development experience, by injecting malicious code to skim customers' financial and personal information from checkout pages of websites. When fraudsters get their hands on stolen credit cards, the most straightforward scam is to purchase goods or services with the stolen credit cards and have them shipped outside the country or to locations where the items can be picked up 'safely' by someone within that fraudster's network. In the case of services, such as food or alcohol delivery, items are often delivered to different addresses and/or often left outside and retrieved (after all, during the pandemic, contactless delivery has become normal for many platforms).

Money laundering

Also known as fake buyer/seller closed-loop fraud, money laundering generally requires a stolen credit card. In this case, often the same person creates a fake 'seller' account and a fake 'buyer' account (or many accounts).

The seller advertises expensive goods for sale and the buyer(s) bids or transacts for those goods with the stolen information. The seller receives the payout from that transaction and moves on to the next. This can happen repeatedly until the credit card limit is reached or the fraud is detected and the credit card is shut down. By the time either of these occur, often the fraudsters have made off with tens of thousands of dollars.

The pandemic has brought fraud to the doorstep of nearly every consumer. The result has adversely impacted the reputation of the marketplaces through which those customers transact. In order to restore lost confidence and maintain those customers post-pandemic, platforms must dedicate resources to identify and prevent fraud. Otherwise, marketplaces will lose the customers that fell into their lap.

About Marketplace Risk: Marketplace Risk is the most comprehensive source of education, networking, and information sharing for the sharing economy and marketplace startup ecosystem to learn risk management, trust and safety, and legal strategy. From our blog, e-newsletter, Platform Podcast, Slack Forum and Webinar Series, to the Marketplace Risk Management Conference, Masters Program, Road Shows and Sharing Economy Global Summit, Marketplace Risk is the most trusted resource for startups taking their businesses to the next level.

www.marketplacerisk.com



Marketplace Risk. **Webinar Series**

Weekly Webinars
Wednesdays at 10am PT

Everything you need to know about...

- 9/23: Leveraging Biometrics for User Identification
- 9/30: Creating Enforceable Terms of Use/Service
- 10/7: Vetting and Screening Your Workforce
- 10/14: The Startup Insurance Landscape
- 10/21: Bridging Online and Offline Risk Gaps
- 10/28: Spam Safeguards and Prevention
- 11/4: Top 10 Myths About Content Moderation
- 11/11: Protecting the Customer Journey from Fraud
- 11/18: Behavioral Biometrics for Trust & Safety

Register for free webinars at:
www.marketplacerisk.com/webinars



About Shaun Packiarajah: Shaun Packiarajah is currently part of the React Investigation Unit as an Intelligence Analyst, specialising in exploring and visualising intelligence data for multiple global brands. Shaun is also experienced in ecommerce, EU policy-making as well as victimisation and criminal justice.

Shaun Packiarajah ■ *Intelligence Analyst* ■ React

The illicit world of counterfeiting is a complex and ever-evolving industry. And it is big business. An **OECD-EUIPO study** into this area estimated that up to 2.5% of world trade is made up of counterfeit and pirated goods. To achieve this scale of trade, the days of counterfeiters setting up shop at the local market have diminished.

Enter ecommerce

The astronomic rise of this form of trade has enabled borderless and anonymous commercial websites – a dream for counterfeiters that enables even more opportunities to market and sell to consumers. When talking about counterfeit purchases, we can divide them into two distinct groups: non-deceptive and deceptive.

Figure 1. Harm Matrix: level of deception versus quality. (Adapted from 'The consumption of counterfeit fashion.' Large, J. (2019))

This article focuses on deceptive counterfeiters and those consumers who are purchasing items in good faith. It also touches upon several example techniques used by counterfeiters to target these users, as well as two example characteristics of consumers vulnerable to these criminals.

Why certain consumers buy deceptive counterfeits

With a focus on consumers unknowingly purchasing counterfeits, below are a couple of scenarios that come into play.

Lack of knowledge regarding products

Consumers nowadays are adept at researching products online, but, sometimes, they don't understand the intrinsic details of that product. This comes into sharp focus with the ongoing COVID-19 pandemic – consumers were expected to wear items such as masks, which often have highly technical specifications. Therefore, how can consumers assess the genuine from the fake? This can also apply to more mundane, yet still technical purchases, such as electronics and auto parts.

Searching for a good deal

Consumers are increasingly getting comfortable with online stores offering great deals (Prime Day, for example). This same feeling can leave them vulnerable if a counterfeiter is sophisticated enough and strategic with product placement.

For example, consumers can identify market value goods alongside established brands on a comparison website. This may convince them they have stumbled onto a special discount. In other instances, counterfeiters will state on their website that they have acquired stock from liquidated businesses or overproduction of an item from a factory.

Techniques used by counterfeiters to target consumers

The following are several identified methods used to defraud consumers by criminals selling counterfeits. →

Linking directly from social media

Consumers often mistakenly believe that offers made through an established social media channel are safe and/or vetted. Counterfeiters use social media tools to target consumers efficiently and quickly earn revenue. This includes consumers looking to purchase genuine products. Should counterfeits engage with the advertising platforms of social media platforms, there are even more tools at their disposal to target consumers.

Creating template online stores

Once an online store controlled by the criminals gains a bad reputation or is shut down, they often simply open another one using a different tradename and adjusting the design slightly. The core of the online store is the same, making this process fast and efficient. These template sites can also operate simultaneously to defraud as many consumers as possible before they are shutdown.

The assurance of trustworthy payment options

Consumers will often rely on the safety of reliable and well-known payment options when looking to buy online. Counterfeiters understand this and prey on this fact. One example is to simply display many well-known payment methods in the footer of the website via logos, as well as false SSL certification, thus making consumer feel reassured to begin the process of choosing their desired product and moving through to the checkout process. Once at the checkout, the actual payment methods on display usually lack strict KYC processes.

Harvesting data

Counterfeit commercial websites have features common to online stores, but for very different reasons, like a newsletter sign-up forms requiring an email address, for instance. Frequently, this is used to harvest data and directly target customers in future interactions.

How to stop consumer's falling prey to deceptive counterfeit offers

As with many forms of fraud, there is no easy answer to this problem. However, by combining and coordinating the efforts of stakeholders involved, this can be tackled effectively over the short-, medium-, and long-term. Below you will find two core suggestions that can push this fight forward.

'Continued growth of ecommerce in the pharmaceutical sector can attract unscrupulous online sellers, leaving patients vulnerable to dangerous counterfeits, so, collaboration across the industry is key.' - Kristian Davey, Intelligence Analyst, Novartis

Educating consumers

By helping consumers understand how to buy safely online, stakeholders can empower them to avoid suspect products. This not only builds trust but also emphasises that consumers can be innocent victims of counterfeiting and that stakeholders are invested in helping them. Examples can include public awareness campaigns, tools to verify sellers etc.

'In order to effectively tackle counterfeiting in the modern age, stakeholders not only need to track the whole supply chain and online presence of these criminals. We also need to investigate the operations in-depth to tackle this global phenomena and protect consumers.' - Ronald Brohm, Managing Director, React

Sharing intelligence

In order to tackle this issue, stakeholders need to work together to make sure information can be shared with those best able to assist with monitoring and enforcement. This can also help identify and target new techniques used by counterfeiters to catch vulnerable consumers. This can include brands, retail partners, law enforcement etc.

About React: React is a not-for-profit organisation, which has over 300 members covering all industry sectors with over 30 years of experience fighting the counterfeit trade. Our network of offices and partners allows us to provide support wherever needed. Members pick and choose the React services: customs, investigations, market, and online enforcement.

www.react.org

Wave Financial

Entrepreneurship and Merchant Fraud in a Post-Pandemic World



About Angie Dobbs: Angie is the Director, Fraud & Risk, responsible for protecting Wave's customers and financial services including its proprietary payments, payroll, and debit card products. Angie holds a Master's Degree in Applied Mathematics & Statistics at the University of Guelph and takes a data-driven approach to risk detection.

Angie Dobbs ■ Director, Fraud & Risk ■ Wave Financial

The effects of COVID-19 on the small business economy has been severe. Being an entrepreneur was a risky endeavour before the pandemic, with approximately **20% of small businesses failing in their first year** all the way up to a 70% 10-year failure rate. It's too soon to tell the full extent of the pandemic on entrepreneurship, but a recent study confirmed that **55% of businesses on Yelp** have shut down during this time. That combined with unemployment at an all-time high which impacts consumers' ability to spend, it's more difficult now than ever to start and run a successful business.

At Wave, we experienced a significant influx of new customers once the pandemic hit, for two main reasons. First, small business owners pivoted to new means of making a living, and therefore had to create new merchant accounts. Second, many left their payment processors after strict reserve policies were implemented to offset the risk of increased chargeback rates which hurt their cash flow. This made legitimate merchants more vulnerable to scams and compromises as they grew more desperate for business.

Merchant fraud is becoming increasingly complex as it evolves through digital channels. It's easier than ever to obtain various sources of stolen data on businesses and their owners, making it far too easy for fraudsters to create new merchant accounts for illicit gains. We've observed a sophisticated trend that combines various fraud types and patience by the fraudster. This layering of stolen data makes it almost undetectable by automated systems and takes a keen eye, sound onboarding controls, and strong underwriting practices to stop.

The fraud type trifecta

We've coined this 'Business Identity Takeover' at Wave, because there are three main fraud types at play. To pull this off, fraudsters must orchestrate a targeted attack on an individual and/or business. This has a lot of moving parts and takes patience to pull off. Each case is a combination of the following fraud types:

1. Identity theft
2. Account takeover fraud
3. Card-not-present fraud

1) Identity theft

The identity of a small business owner is targeted. It's easier to make the payments account appear legitimate if you assume the identity of an existing business as opposed to creating a fictitious one from scratch. You then already have a strong social media presence, often with positive reviews, and good online history. →

2) Account takeover fraud

In the most sophisticated cases, multiple financial, social, and email accounts that belong to the true business owner or employees are taken over by the fraudster, making the account appear more legitimate. This is typically done through phishing attacks to employees of the targeted business, which then allows the fraudster to gain access to:

- Email: the real inbox of the business may be taken over, but if that's not successful, they will create a new but seemingly close email address that is easily overlooked.
- Bank account: being able to gain access to the business' online banking credentials is highly valuable. Alternatively, the fraudster may open a brand-new bank account in the name of the business owner, employee, or business.

3) Card-not-present fraud

Stolen card data is used to make online payments to the fraudulent merchant. Typically, we see card data that is stolen from the same geographic region of the business as well.

The key to detection

Strong controls and thorough underwriting of the merchant and their clients is imperative to detecting this type of fraud. You must connect all the dots. Since most of the data provided will revert to the true business owner, it's important that your analysts and systems pay attention to what doesn't match. If something seems off, consider secondary verification. Nothing is foolproof, and you need to balance operational capacity with fraud detection.

It may not be cost-effective to put all your effort into detecting the fraud at signup, as often the most influential data is found on the cardholders when the 'merchant' begins to receive payments. It is a judgment call to balance operational capacity, fraud losses, and customer experience that must align with the priorities and risk appetite of your business.

At the end of the day, the goal is to waste the fraudsters' time enough that they give up on attacking your platform. This trend takes lots of patience and time to pull off, which means it can successfully be curbed by making it too tedious with little payout for the fraudster.

About Wave Financial: Wave Financial's award-winning software solutions help small business owners manage their finances. Wave provides accounting, invoicing, payroll, banking, and payments software, as well as bookkeeping services, built into a comprehensive platform. Wave has won numerous awards for growth, innovation, and company culture, including Deloitte Fast 50, Deloitte North American Fast 500, KPMG Fintech 100, CB Insights Fintech 250, Canadian Innovation Awards (Financial Services), Canada's Best Workplaces, and more.

www.waveapps.com



Technologies and Innovations That Keep Fraudsters at Bay

Having a powerful fraud prevention suit is a must in the commerce world. This is why it is very important for businesses to be up to date with the newest technologies and best practices they need to employ in order to not only improve their existing risk management strategy, but also to be ready to prevent any emerging type of fraud. Notable key players in the industry discuss in this chapter about key techniques to fight fraud, manage risk, eliminate pain points, and adapt to customers' expectations.

Cybersource

Staying Ahead in a Changing World: Building Fraud Strategies That Get More Business In



About Mark Strachan: Mark is the business owner for the EMEA Managed Risk portfolio at Cybersource and a fraud risk professional with over 12 years of experience. He works with enterprise clients on fraud strategies to reduce risk and optimise revenue.

Mark Strachan ■ *EMEA Managed Risk Principal* ■ *Cybersource*

Adapting to change certainly isn't anything new for ecommerce businesses, but change is happening faster than ever before as customer and fraudster behaviour evolves, new regulations become effective, and other external factors come into play. The challenge for ecommerce businesses is to keep pace and adapt their fraud strategies accordingly. Of course, they need to keep fraud and the associated chargebacks under control. But the other side of the fraud management coin is about accepting as many good orders as possible to keep customers happy and loyal, and bring in more business.

Machine learning is powerful. Adding human insight makes it more powerful

We've seen that merchants whose fraud screening solutions rely solely on machine learning (ML) can soon fall behind during turbulent times. Although ML is a powerful technology, it works based on historical data. Thus, it's only as good as the data it consumes and the human-set rules it works to. It may be slow to pick up on radical changes in consumer and fraudster behaviour, which can leave a merchant experiencing:

- high rates of fraud and chargebacks; or
- low levels of customer satisfaction as too many good orders are rejected.

On the other hand, merchants whose fraud screening tool is backed by experts able to help with fraud strategy are often faster to adapt. They can take advantage of human intervention to analyse new trends and adjust fraud screening rules accordingly.

During the pandemic, for example, airlines had to act quickly to ensure they could accept one-way bookings for repatriation flights.

They had to change rules that would normally flag one-way bookings as potentially fraudulent transactions, so that people could buy tickets to fly home when lockdowns or quarantine restrictions came into force.

The other thing to bear in mind is that it's unlikely that any individual merchant will have all the answers. That's when gleaning intelligence from external sources comes into its own. Peers, merchant associations, and suppliers will all have insights to share about new trends and behaviours that can help individual merchants refine their own approaches.

Shift the focus: identify the good guys

One thing we're seeing more and more is that fraud strategies really are becoming more sophisticated. Savvy merchants who are already doing a good job of keeping the bad guys out are now actively focusing on ways to get more business in.

To do that, they're examining the customer experience and aiming to make it smoother and more enjoyable – for both new and returning customers. They're also getting to know their customers better, understanding their habits and preferences, and adding personalisation to their shopping journey. To do that, your fraud strategy needs to be able to recognise genuine customers so that you can roll out the virtual red carpet for them. If you make it easy and convenient for them to buy from you, there's every chance they'll keep coming back.

Ultimately, you need to treat good customers with different rules in your fraud screening solution than those you use for suspicious-looking transactions. →

There are plenty of elements you can use from your own and third-party data. Behavioural biometrics and device fingerprint are especially powerful sources of information.

The fraud manager's role is changing

This shift in focus naturally means that the fraud manager's role is evolving, too. Although identifying and preventing fraud remain key objectives, fraud managers are becoming closely involved in efforts to improve the genuine customer experience and turn away fewer good orders.

In fact, many merchants now view fraud management as a higher-value, more strategic activity than before, and are weaving it into the fabric of their business. They're using the data that fraud management teams collect to help identify changes in customer behaviour and purchasing patterns, and support sales strategy formulation.

The next step: recapture lost revenue

Merchants who have fraud under control with a flexible strategy that also optimises the customer experience may now be thinking about other ways to help increase revenues.

One avenue to consider is the fact that issuers generally decline more card-not-present (ecommerce) transactions than card present (in store). Given that some of those declined transactions will be good orders, this represents potential lost revenues.

So that fewer good orders are declined, merchants may want to find ways to help issuers make more informed decisions. This could be achieved by merchants screening transactions for fraud before submitting them. That way, issuers will receive better quality

transactions that they're more likely to accept. EMV 3-D Secure 2.x can also help here, as it allows merchants to share 10 x more data with issuers compared with 3DS 1. It will also provide issuers with the way to challenge and authenticate the payer, if they find the transaction risky.

Conclusion

To keep pace with change and bring in as much business as possible, ecommerce businesses should ensure they:

- have a fraud management approach that's agile enough to respond to evolving customer and fraudster behaviour;
- can recognise good customers and give them a great shopping experience.

Looking ahead, they may also want to consider developing additional strategies for maximising revenues. Cybersource has developed a vision for the next generation of ecommerce payments and fraud management that includes initiatives for recapturing lost revenues. To find out more, [download](#) our 'Revenue Capture' white paper today.

These materials and best practice recommendations are provided for informational purposes only and should not be relied upon for marketing, legal, regulatory or other advice. Recommended marketing materials should be independently evaluated in light of your specific business needs and any applicable laws and regulations. Visa is not responsible for your use of the marketing materials, best practice recommendations, or other information, including errors of any kind, contained in this document.

About Cybersource: Cybersource helped kick start the ecommerce revolution in 1994 and haven't looked back since. Through global reach, modern capabilities, and commerce insights, we create flexible, creative commerce solutions for everyday life – experiences that delight customers and spur growth globally. All through the ease and simplicity of one digital platform to manage all payment types, fraud strategies, and more. Knowing we are part of Visa and their security-obsessed standards, you can trust that business is well taken care of – wherever it may go.

www.cybersource.com

[Click here for the company profile](#)

Fraugster

Balancing preventing fraud while accepting good transactions – Max Laemmle, Founder & CEO of Fraugster, reveals best practices on how businesses can increase approval rates.



About Max Laemmle: Max is the CEO and Founder of Fraugster, an AI-driven fraud prevention company. Prior to founding Fraugster, Max co-founded Better Payment, a German payment gateway service provider, and also acted as the product evangelist for the mPOS company SumUp.

Max Laemmle ■ Founder & CEO ■ Fraugster

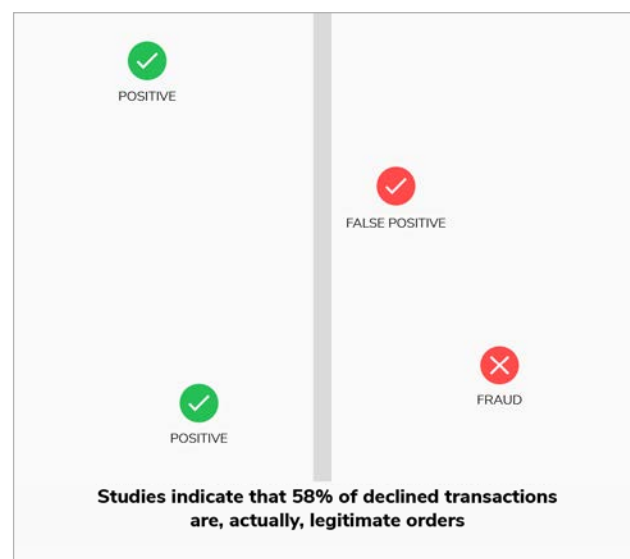
When tackling fraud, there is always a high percentage of quality transactions that are falsely declined. How can merchants eliminate fraud without accidentally blocking good customers?

When it comes to approval rates, there is a limited amount of data points that merchants can use to base their decisions on. And if businesses don't fully utilise the data, they could be rejecting legitimate transactions because their anti-fraud technology isn't agile enough. Due to outdated technologies, merchants across industries are now seeing record losses because of fraudulent actions and the increase in false positives. It is more important than ever to ensure that your fraud prevention system understands the buyer's true intent and can make considered decisions on each transaction attempted.

“ Merchants require more adaptive approaches to differentiate between good and bad transactions. And this is where Artificial Intelligence can play a big part.

Fundamentally, this comes down to the information that needs to be collected. Data, such as IP addresses, email addresses, and payment methods, combine to paint a picture of your online transactions' validity. However, more and more businesses find that these assets don't always tell the whole story. Merchants require more adaptive approaches to differentiate between good and bad transactions. And this is where Artificial Intelligence can play a big part.

With Fraugster's proprietary AI-technology, each transaction's behavioural pattern is analysed in real time, leading to an accurate decision. This has the benefit of delivering a frictionless customer experience without letting bad transactions slip through.



How can Artificial Intelligence spot the difference between a potential fraudster and a legitimate customer in real time?

The AI performs at a rate comparable to thousands of excellent risk analysts. So, if a customer attempts a transaction, all of their data points are sent to the AI-Engine for inspection. Here, the AI enriches the data, investigating each piece of information and comparing it against others to determine whether it is suspicious. Does the username match the email? How many times has this credit card been used for a purchase on this site? Within what time frame? →

On their own, individual data points can't tell us the whole story. For example, one shipping address could be connected with two different credit cards. This doesn't mean that it is fraudulent, it could simply mean that it's a shared living space. But when the AI-Engine consolidates all of this information together, a better understanding of the story emerges. Like a detective building a case of evidence, the AI-Engine evaluates thousands of connections and attributes, looking for possible patterns, mismatches, or irregularities.

From here, the AI-Engine presents a Fraud Score, and a transparent and traceable determination is reached: 'Is this a good transaction or a bad one?' or, 'Is this a real customer or a fraudster?' And because a team of real fraud analysts has taught the AI-Engine to mimic their thought process, the Engine can now perform this analysis on every single transaction in less than 15-milliseconds.

So, the merchants who work with an AI-based fraud prevention solution now have the accuracy of a human analyst and the speed and scalability of a computer, which they require to grow their business while protecting it from ongoing threats.

How can merchants maintain high approval rates in the PSD2 world?

While PSD2 attempts to provide a more secure experience for customers, the SCA (Strong Customer Authentication) requirements introduce a new set of challenges. While it does reduce the risk of fraud within the European Economic Area (EEA), it also creates a more complicated payment experience for the customer. Tests carried out by payments consultancy CMSPI suggest up to 30% of sales could be at risk because frustrated customers abandon baskets at checkout and because 3DS2 solutions are not working effectively. Customers want a safe, secure checkout experience but without

additional friction or waiting times. But how can merchants present an acceptable balance of both, seemingly opposing, demands? It comes down to merchants understanding the regulation. And specifically, knowing what exemptions they can raise while remaining compliant. For instance, PSD2 states that exemptions can be raised for a variety of circumstances. These include recurring payments, low value, and low risk (often referred to as Transaction Risk Analysis). Coordination with PSPs and acquirers is the key to success here. Firstly, it is important to liaise with your PSP in advance to know their fraud level and understand their dependencies with their acquirer. Then analyse your current flow and forecast where you have the highest probability of raising exemptions. For instance, PSD2 allows exemptions up to EUR 100 if your fraud rate is under 0.13%. A potential best strategy for merchants could be: keep a low fraud rate to exempt low risk transactions.

The merchants who have this balance will see a dramatic improvement in their authorisation rates. And the best way to execute this strategy is a focused effort with an integrated fraud detection solution.

About Fraugster: Fraugster is a fraud prevention company, which helps online merchants maximise their revenues while reducing operational costs. Fraugster serves clients across industries: from online retail and marketplaces to gaming and travel. Fraugster operates globally and serves merchants both directly and through payment companies, minimising the integration effort.

www.fraugster.com

[Click here for the company profile](#)

Kount

Three Keys to Protect and Scale Ecommerce in 2021



About Rich L. Stuppy: For more than a decade Rich Stuppy has been involved in developing fraud mitigation, compliance, and big data strategies. In his role as Chief Customer Experience Officer, Rich is responsible for client success, data analytics, and ensuring Kount's users have the best customer experience. Collaborating directly with customers, he works to inform Kount's product roadmap, identify new and emerging threats, and drive innovation for ultimate customer satisfaction.

Rich L. Stuppy ■ *Chief Customer Experience Officer* ■ Kount

The events of 2020 have permanently altered the way customers engage with businesses. Looking to 2021 and beyond, digital businesses must adapt, expand, and innovate to stay relevant and profitable in the new environment. For ecommerce businesses, it will become even more critical to enable new revenue channels, protect against chargebacks and fraud, and enhance the entire customer journey. Understanding identity trust, or the level of trust or risk behind every interaction, is key to scaling in these three key areas.

Innovate and protect new revenue channels to pace with digital acceleration

In the past year, consumers have embraced new digital channels more than ever before, including mobile order ahead, Buy Online, Pick Up in Store (BOPIS), curbside pickup, and similar models. While some shoppers may be back to browsing the shelves in store, many still count on contactless methods, and no matter their preference, consumers will expect these offerings to continue to be offered into the future.

Successful BOPIS (or Buy Online, Pick Up Curbside, or any other of similar acronyms), requires timely processing and minimal customer interaction. There is little to no time for manual review of an order, and additionally, this model also accelerates card-not-present (CNP) payment transactions, which shifts the liability to merchants. Even just sitting in their cars in the parking lot, a few yards away from the traditional point-of-sale, shoppers are making their orders online, making it a CNP interaction.

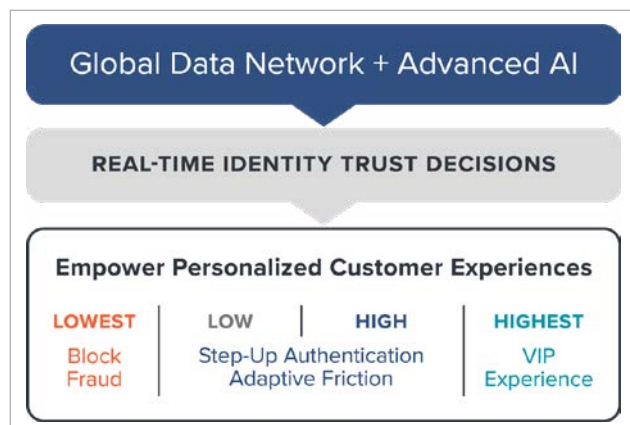
With these changes, businesses are tasked with balancing digital fraud protection measures with customer friction to ensure all channels are adequately protected. There are several points along the customer journey where businesses can monitor and assess risk, as well as validate the customer making the purchase. Kount's AI-driven fraud prevention coupled with the Identity Trust Global Network and its highly customisable platform enable businesses to protect and grow this channel in a way that is seamless to their good customers.

Level up fraud protection by establishing the level of identity trust behind every interaction

With the increase in ecommerce, fraud and chargebacks inevitably follow. Fraudsters go where the money and data are, and they know digital experiences are a prime opportunity.

It's not enough just to stop bad transactions – businesses must also maximise revenue and approve as many good orders as possible, as quickly as possible. That requires establishing Identity Trust – the level of trust or risk for each identity behind every payment, account creation, or login event. Real-time identity trust recognition allows businesses to personalise customer experiences across the spectrum of identity trust – from frictionless VIP experiences to blocking fraud.





By linking signal data from 32 billion annual interactions across 250 countries and territories, 75+ industries, 50+ payment processors and card networks, and decisions from thousands of fraud analysts, Kount's Identity Trust Global Network blocks payments and account takeover fraud in real time, and enables personalised customer experiences.

By having a deep data set, Kount's AI provides visibility and intelligence far beyond the limited data available to a single company or industry. The results are immediate, including low false positives, high automation, low manual reviews, personalised customer experiences, and frictionless customer interactions – all of which grow revenue, especially during this period of digital acceleration.

Earn repeat customers and protect the brand by detecting bot attacks at any point in the customer journey

Digital innovation means businesses are introducing new ecommerce experiences, channels, and offerings. Each of these points offers an opportunity to deliver exceptional experiences to good consumers – ideally creating loyal, repeat customers. On the other hand, each of these points on the customer journey introduces risk and potential for fraud and malicious bots, which look to exploit any vulnerability to steal payment information, stored valued, personal information, and more.

From account creation, to login, to payment interaction, businesses need to implement adaptive protection to stop malicious bots, allow desirable bots, and quickly analyse, classify, and adapt policies towards new and questionable bots.

Kount's complete view of the customer journey allows it to establish a baseline of normal behaviour, and then to quickly identify abnormal, high risk behaviour. By expanding bot prevention and detection from checkout to earlier points in the customer workflow, Kount offers an advantage that is critical to mitigating the cost of bot attacks on business and customers, as bots can attack multiple points in the digital journey.

About Kount: Kount's Identity Trust Global Network delivers real-time fraud prevention and account protection, and enables personalised customer experiences for more than 9,000 leading brands and payment providers. Linked by Kount's award-winning AI, the Identity Trust Global Network analyses signals from 32 billion annual interactions to personalise user experiences across the spectrum of trust — from frictionless experiences to blocking fraud. Quick and accurate identity trust decisions deliver safe payment, account creation, and login events while reducing digital fraud, chargebacks, false positives, and manual reviews.

www.kount.com

[Click here for the company profile](#)

Kevin Lee, Trust and Safety Architect at Sift, reveals for merchants and fraud management teams the importance of control and transparency for Digital Trust & Safety.



About Kevin Lee: Kevin Lee is a Trust and Safety Architect at Sift who helps customers implement strategies that cross-functionally align risk and revenue programs. Prior to Sift, he has spent the last 14+ years leading various risk, chargeback, spam/scams, and trust and safety organisations at Facebook, Square, and Google.

Kevin Lee ■ *Trust and Safety Architect* ■ Sift

Merchants have started to offer more flexible shopping options, such as Buy Online, Return in Store (BORIS), and BOPIS, for example, in a bid to consolidate the omnichannel experience for their consumers. How have fraudsters exploited this move?

Fraudsters have already taken advantage of BOPIS because:

- a) this is a new channel that many merchants just launched (or significantly expanded) due to COVID-19. With many newly launched fulfilment options or functionalities, risk mitigation isn't always the business' focus. Fraudsters are often the earliest adopters of new features and flock to where they see the potential for financial gain;
- b) in the past, fraudsters would take advantage of delivery options like next-day shipping in order to get online orders fast. Trust & Safety teams would often see this as a risky signal. Now, the expectation is that all BOPIS orders should be fulfilled and ready for pick up in a few hours. This gives the merchant very little time to do fraud screens when conducting manual review. In general, merchants don't want to risk a negative customer experience so they will err on the side of fulfilling the order;
- c) during the physical pick up, very little verification is done. Buyers are usually wearing face masks so it's difficult to verify identity.

With the significant growth of ecommerce purchases, a seamless transaction is just as important as a secure one. What are the best practices to enrich transaction details so as to avoid false positives, chargebacks, and boost customer experience?

Merchants must deploy checkout flows that have dynamic friction. Knowing that 99%+ of transactions are from legitimate customers, merchants should enable 1-click (or nearly 1-click) checkout for these customers. Every extra click and keystroke compromises customer conversion rate.

“ *Merchants must deploy checkout flows that have dynamic friction. Knowing that 99%+ of transactions are from legitimate customers, merchants should enable 1-click checkout for these customers.*

Merchants should only introduce friction (like having the customer enter in a CVV code) less than 1% of the time. Obviously, this takes a highly accurate machine learning driven system to know when to dynamically introduce this friction. This dynamic friction can become a competitive advantage for a merchant.→



Sift has pioneered the Digital Trust & Safety approach in 2019. What is the value proposition of it now, with all these shifts in customer behaviour and fraud attempts increases, and why should businesses embrace it?

Sift launched the Digital Trust & Safety approach at the beginning of 2019 because we have seen consumer expectations and fraudulent attack vectors shift considerably over the last few years. Within the last year, we've seen a surge in payment fraud, account takeover, and content abuse. In fact, we just released a [report](#) showing the account takeover rates have increased 282% in the last year, and that rate has accelerated even more during the pandemic. It's clear that consumer expectations and fraud are running in parallel with each other and as consumers adopt easier ways to transact, fraudsters exploit those channels. The value proposition of Sift is simple: allow every legitimate consumer to seamlessly interact on a website while dynamically introducing friction for malicious users. This can only be done at scale and with high accuracy with exceptional technology, tools, and data.

Fraud management teams are sometimes perceived as cost centres. How can these teams increase visibility and control of their fraud prevention operations?

In order to increase team visibility, try and align incentives of the risk team to company level goals. If your company has a goal of launching a new product or feature, how can the Risk team help make that happen? For example, if your company runs a marketplace that pays out merchants on your platform, what if the Risk team was able to unlock an instant payout feature without increasing losses?

The highest performing Risk teams that I've seen actually increase revenue for the company. How? They enable the company to grow faster, launch more products, and to reach customers that other competing businesses cannot reach. These Risk teams understand when, where, and how to dynamically apply friction to the user experience. The results are higher customer conversions and reduced/controlled losses. This is how the Risk team can become a competitive advantage and drive more value for the company.

The Q4 of 2020 is one of the most challenging period merchants have ever faced: handling more online purchases and extra costs in some departments, preparing for the sales season, and, in some instances, getting ready for SCA compliance. How does Sift support its merchants in dealing with all these challenges?

Sift enables companies to focus on what they are best at, delivering great products, experiences, and services. Risk and fraud should not have to weigh on the minds of these merchants, and that includes configuring SCA. Sift has built industry leading machine learning technology, tools, and data networks that allow merchants to scale and automate without risk.

About Sift: 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 35 billion events per month, and a commitment to long-term customer partnerships.

www.sift.com

[Click here for the company profile](#)

Simility

Why Explainability Is Key to Success in Machine Learning



About Sean Nierat: Sean is a Product Marketing Manager at Simility, a PayPal Service, where he leads marketing direction and strategic vision for Simility's Large Enterprises Ecommerce solution. Prior to this role, Sean spent time at McAfee and Intel helping drive cyber-focused marketing efforts.

Sean Nierat ■ Product Marketing Manager ■ Simility, a PayPal Service

Machine learning (ML) is part of a burgeoning AI industry that could soon become a multitrillion-dollar opportunity for global businesses. It is being used by Simility, a PayPal Service, and others to help pioneer advanced data-driven fraud prevention by enhancing human intelligence with a 360-degree view of each customer. Yet, as ML becomes ubiquitous, it's increasingly being argued that we not only need systems to make accurate predictions but also ones that explain why they've arrived at a particular answer.

Tackling bias with transparency

We've come a long way from the old days of fraud prevention. It's undeniable that the bad guys are getting smarter, with huge volumes of readily accessible customer data at their disposal and a wealth of tools bought on the dark web. Sophisticated fraud built on these foundations demands an equally sophisticated response. That's why Simility uses best-in-class ML to continually optimise the complex rules written by our client's in-house fraud and data science teams, and to apply these rules to large datasets in order to spot patterns that humans may miss.

The problem with such systems is that they're only as good as the data they're trained on. Increasingly, organisations are concerned about unconscious bias emanating from this data, and the algorithms designed to interpret it. With ML used today in everything from mortgage application approvals to police facial recognition systems, there are important questions to answer – especially in a new era of intense regulatory scrutiny.

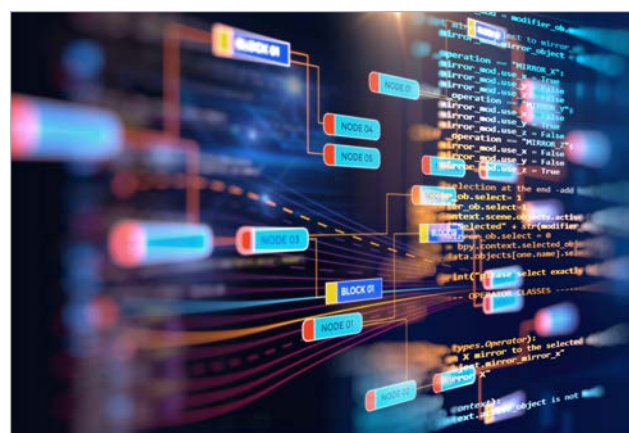
Clear box vs black box

This is where clear box ML or 'explainable AI' (XAI) approaches come into their own. Black box models like artificial neural networks

(ANNs) or deep learning operate so that even the humans that designed them don't know how decisions are made. However, with XAI, businesses gain vital insight into the whole process, from data collection to decision making.

This additional clarity and transparency offer multiple benefits including:

- improves business confidence in an XAI-powered prediction/outcome;
- enhances the ability to control and manage algorithms in line with business objectives;
- increases accountability, as systems can be audited;
- improves regulatory compliance efforts;
- enables teams to identify new fraud patterns faster.



A new approach

Simility's enterprise offering champions clear box, best-in-class ML through our use of explainability methods like LIME, Shapley, and RL-LIM. Our prediction engine delivers an interpretability plot for every single event, helping to drive customer confidence in the →

results and continued ongoing improvements.

Our platform is purpose-built to handle both the complex fraud challenges businesses face today and to make the necessary adjustments to help address those of tomorrow. With Simility, businesses can take a dynamic approach to fraud – streamlining the experience for good customers and adding protection layers when necessary.

Simility leverages the fraud and risk knowledge from the PayPal 2-Sided-Network of over 346 million active accounts transacting 12 billion times a year as well as integrated third-party feeds to enable the processing and correlation of vast amounts of heterogeneous data to help deliver actionable business intelligence.

Here's how:

- a purpose-built data lake stores structured and unstructured data from various sources;
- powerful Device Recon analyses hundreds of mobile and desktop device characteristics and behaviours, and applies machine learning models for risk scoring and clustering;
- easy-to-update rules and machine learning algorithms help businesses adapt to changing fraud schemes;
- robust link analysis and data visualisation help enable businesses to proactively uncover anomalous patterns indicative of fraud;
- real-time complex authentication helps differentiate trusted from suspicious users.



About Simility: Simility offers real-time risk and fraud decisioning solutions to protect global businesses. Simility's offerings are underpinned by the Adaptive Decisioning Platform, built with a data-first approach to deliver continuous risk assurance. By combining artificial intelligence and big-data analytics, Simility helps businesses orchestrate complex decisions to reduce friction, improve trust, and solve complex fraud problems. Built by industry veterans, Simility is trusted by some of the world's leading consumer brands across financial services, payment processors, and commerce merchants.

www.simility.com

[Click here for the company profile](#)

The Problems With the Fraud Proof of Concept and a Possible Solution



About Liam Castagna: Liam Castagna is Head of Payment at Insparx GmbH. He is responsible for their Payment and Fraud vision and works tirelessly to optimise the payment flow. As a committed dataphile, he believes leveraging your own data is the most effective way to build business performance.

Liam Castagna ■ *Head of Payment* ■ Insparx

Evaluating a new fraud solution provider can be difficult. No two merchants are exactly the same; what you sell, how you sell it, who your good customers are, what fraud challenges you have, and your risk appetite – all play a part in making your challenges unique. As part of the evaluation, you will want to know how the solution performs on your data. This means integrating and running a Proof of Concept (POC).

The testing part

Testing a fraud provider on your system is expensive. Every ROI is compelling, every new technology is sparkling with possibility and every hosted dinner is flavoured with success stories, but merchants don't have endless integration budgets. We would all like to test the newest and greatest providers against our incumbent, but usually, resource constraints mean our wish list is reduced to a (very) shortlist of solutions we can try. Where there is no tangible risk to the business, often resource constraints reduce the list to zero.

Usually, when testing a new fraud solution, there is already an incumbent in place. The challenger solution is integrated in silent mode and both run side-by-side. Solution providers set the integration bar as low as they dare, knowing that once integrated, the scales are heavily weighted in their favour. Even if they don't live up to expectation, as long as they outperform the incumbent solution, they can be confident they will be adopted. A merchant is unlikely to have the resources to repeat the process to achieve further efficiencies in performance or price. These bare-bones integrations can cause problems. When performance is not as expected, the limitation of the integration can be cited as the problem. This leaves the merchant having to evaluate the solution on unproven future performance expectations.

Running a strong Proof of Concept test goes a long way to mitigating these problems. Once it has been agreed to do a Proof of Concept, discuss again with the fraud solution provider what they will need in order to be confident of their performance, how deep an integration is needed, and for how long it should run. A more generous POC will give more accurate results. However, it will take more resources, so now the merchant has even less resources to test multiple providers.

Considering a payment orchestration provider

The industry has proposed a different solution and it shows a lot of promise. The orchestration provider is a fairly new concept in the world of payment services. The orchestration layer is the infrastructure in a merchant or an agnostic third party that connects a range of different solution providers to the merchants' system. It is sometimes hard to argue they currently provide a little more than the old style 'full stack' or 'full service' PSPs, where a payment gateway will offer all the basic services required for processing payments. However, the potential (and the marketing literature) looks good, and in the area of fraud, this could be a game-changer. With all the fraud solution providers available through one standardised API, a merchant with limited resources has the ability to make sure it always has the best solution.

When integration fees and integration effort are removed from the Proof of Concept, merchants rush to regularly testing the market to see what new and innovative providers can offer. I personally look forward to the day when we can report to our bosses: we 'know' we have the best the industry can offer because we run continuous back-to-back tests of incumbent vs challenger. →

With the barriers to switching between solution providers reduced to an experience similar to switching acquiring banks, we can expect a more accurate market valuation of the fraud service. Why would a merchant pay more when a new disrupter fraud service provider can achieve the same performance for less? This environment will benefit to market solution providers and encourage innovation. Via the orchestration provider, new providers can easily access a large number of merchants. Instead of investing in large marketing budgets to raise their profile and gaining visibility (and perceived respectability) in the industry, they will be able to connect with merchants via the orchestration layer and let the results speak for themselves. The merchants are able to try the newest and innovative solutions and the provider gains direct access to the market to prove their product.

These fraud orchestration layers have some hurdles to overcome. Standardising data between the merchant and the solution provider is challenging. A wrong implementation will limit how a solution provider can tailor a service to an individual merchant. The business model needs to be sold to both the solution providers as well as the merchants. The benefit to merchants is clear but the solution provider needs to recognise the growth potential. My assumption is that it will be adopted by those who are confident their product is the best performing for some merchants as well as by new solution providers looking to get into the game. The barriers to changing providers may be considered by the solution providers as a benefit to their business model; it will be interesting to see which route the big players take.

While we wait to see if fraud orchestration matures into the solution we hope for, we, merchants, are left considering our limited resources wisely, valuing our incumbent relationships and choosing our challengers carefully.

About Insparx: Based in Munich Germany, Insparx GmbH is a leading global online dating merchant in over 40 different countries. With a fully subscription business model they are experts in customer retention and managing an extended payment lifecycle.

www.insparx.com

STRATGranat

Automation: An Enabler to Run a Marathon or Sprint



About Catherine Tong: Catherine is an independent fraud, risk, and payment specialist with STRATGranat. Previous projects include complex fraud investigations, Global internal audit programmes, and setting up and managing ecommerce fraud and payment teams. She has also served as a European Board member for the MRC and is currently an Ambassador for the European Women in Payments associations.

Catherine Tong ■ *Independent Fraud, Risk, and Payment Specialist* ■ STRATGranat

2020 has been the year where we have all been asked to become athletes, as speed, agility, and focus have been important in our professional lives – also discipline and determination in many of our personal lives – but in general, drive and resilience have been important to keep us going, as well.

In ecommerce, speed and agility have long been capabilities which most businesses have strived for. However, what has taken many companies by surprise is that what felt like speed before has now been turbo-powered and projects expected to take 12-18 months have been delivered in the last 3 – proof that with the right focus and collaboration, great things can happen. Never before have companies been required to embrace digital transformation so aggressively to at least try and keep up.

In the fraud and payments space, this has certainly been true, particularly in industries such as retail, where volumes have moved from physical stores to ecommerce, and many new pressures are faced with one common theme – the need to automate. Businesses have simply not had the time and often money to increase or retrain people, or to change systems, thus those who already had a strong sense of automation have been more agile and able to adapt.

For fraud and payments, machine learning is often at the heart of automation

The automation of fraud decisions is made up of various algorithms making the binary decision of whether customers are able to complete their purchase or not. It is theoretically possible to fully automate this process, however, many would argue that a human is

needed to drive accuracy in the true 'grey areas', through a manual review or as a sense check where purchasing behaviours suddenly change. In this instance, automated machine learning does most of the heavy lifting, and gives a company the ability to scale the human element through new hires or retraining existing staff, meaning continued employment for those who would otherwise have lost their jobs. The manual review team and fraud manager play an important role as they remain the eyes and ears of sudden fraud attacks, but their scale is likely to adjust, as machine learning removes more of the genuine transactions from analyst workloads, allowing them to focus on the true grey areas, but also to manage alerts triggered by the machine learning if there are spikes in decisions not previously seen – the 'sense check'.

Understanding the type of models used and how they behave will also impact the ability to automate. Some machine learning models themselves have also been subject to a decrease in accuracy and therefore required retraining. Other models, which avoid the concept of 'over-fitting', will naturally adjust to these changes, but require a human 'sense check' of what is going on in the wider industry or world. Again, the human touch should not be entirely eliminated.

In payments, automation is more complex as it is not a binary decision. For those who leverage machine learning to route their payments traffic, they want to optimise acceptance rates and minimise their processing costs, by moving quickly and with minimal human intervention. →

This means that there has to be some human intervention and - although some tools are marketed as giving automation through machine learning - they are in fact human-dependent rules in the background (to manage volumes sent to different vendors, for example).

For both fraud and payments, companies will always benefit from having an automated backup plan. For example, for payment processing outages, an automated backup plan will be having the ability to automatically switch payments traffic to a new provider and ensure that customers and associated revenue are not lost.

Testing out new features and functionalities also offer a great use case for automation

With A/B or multivariate testing, making adjustments to the checkout page or payment offers can take a lot of time and effort to manage effective samples and reporting. Now that there are many tools on the market, once the hypothesis is clearly defined, the variations can be left to run so that the statistical analysis will lead to data-driven results and the business can focus on the outputs and decision-making to optimise their customer experience and conversion.

Automation does not remove the role of people altogether, as done well, it should empower people to be more focused and effective. However, the bias people can bring may damage company performance, as well as the fact that people have their own motivations and ways to work. Therefore, positioned well, these will propel a business forwards, while positioned badly, you could end up with empire builders and parochial views, which slow a business down and cause duplication. Machines do as they are told, but a machine is only as good

as its inputs. If we relied fully on these services, over time, they would deteriorate as they fail to take into account changing business models, consumer purchase patterns, and other innovations. Consequently, having some specialist manual intervention, at least from time-to-time, is still important.

In recent months, we had to adapt our skills to be able to switch from marathons to sprints and back again, but it has proven that automation supports this switch and those who have mastered the collaboration between people and automation are winning. Those who have found an appropriate balance are also those who are more likely to succeed in the long-run as people can run a marathon, but not multi-marathons back-to-back, and they certainly can't sprint for as long as a marathon. Having the right automation to support the journey will mean that eventually they will go further. Do you have the right automation?

About STRATGranat: STRATGranat aims to be the Payment sector service company. It supports fast growing payment sector companies with a very horizontal portfolio of 100 packaged services, Strategic, Operational or HR related. Its credibility is based on 25 experts with more than 15 years of experience in their fields, who have worked for 100 tier-1 companies.

www.stratgranat.com

Summit Partners

AI-based Intelligent Verification and Authentication Are Coming



About Ralph A. Rodriguez: Ralph is an Executive-in-Residence at Summit Partners where he works alongside Summit's technology team to identify new opportunities within growth stage technology companies. Previously, Ralph was an MIT Fellow and a Research Scientist at Facebook where he led Applied Identity and Intelligence. Prior, he was the Co-Founder and CTO of Confirm.io, which Facebook acquired in 2018. As the longest-serving Fellow at MIT, he pioneered research on AI, cloud, mobile, neural science, and security at the MIT Media Lab and Harvard-MIT Health Sciences and Technology (HST) department.

Ralph A. Rodriguez ■ Executive-in-Residence ■ Summit Partners

Digital identity, remote consumer enrollment, biometrics (physical and behavioural), risk and identity assurance solutions, as well as downstream reauthentication solutions, have been leading the pack for global enterprise spend over the last few years. The global COVID-19 pandemic has served to further highlight the importance of these solutions. The rapid transition to a work-from-home environment necessitated an equally rapid IT education for employees caused a ripple effect across the identity ecosystem forcing enterprises to provide safe and secure solutions that enable employee access to critical resources and systems as if they were sitting at their in-office workstation. For significant consumers of digital services such as banking, insurance, and healthcare, the ability to create new online accounts and remotely verify online identity is paramount to gain access to critical services in a COVID world.

This need to provide a safe and secure way for employees to gain access to data, communication, and collaboration tools – as well as for consumers to access services – has been a new sales goldmine for the many identity solutions and providers as of late. But, at what cost?

For the enterprise, identity solutions present yet another vendor to onboard and manage, a new workflow for IT departments to implement and integrate into their corporate systems, and a potential new set of vulnerabilities for the CISO's team to watch. For enterprises operating in regulated industries, including banking, finance, ecommerce, gaming, healthcare, and

the broader 'sharing economy', the primary enterprise stress is driven by the need to solve and manage digital enrollment. These businesses must address the proverbial 'are you who you say that you are?' question and demonstrate compliance with Know Your Customer (KYC) and Anti-Money Laundering (AML) rules. This required identity management causes consumer friction, which can impact the business units (BU) who are focused on increasing sales with new customer growth and providing consumer services, while at the same time protecting consumers against both identity and financial theft, fraud, and loss of personal or private information. These same solutions to protect consumers can also impact the consumer experience and lead to a negative experience, consumer drop off, and the loss of revenues, from new and existing consumers switching to competitors who have better digital workflows and consumer experiences.

Digital identity point solutions

There are a myriad of point solutions being marketed for identity management:

1. Anti-Money Laundering (AML);
2. Know Your Customer (KYC)/Know Your Business (KYB);
3. ID verification;
4. Facial ID match;
5. Genuine assurance identity;
6. Device ID/GEO ID match;
7. Mobile network operator (MNO) match;
8. Face finger voice biometrics;
9. Behavioural biometrics; →



10. Passwordless login;
11. Fraud risk assessment;
12. Credentials & blockchain;
13. Artificial intelligence-based fraud detection;
14. Identity hardware;
15. Identity platforms (orchestration).

What is most interesting is that many of the companies in each of these categories have partnerships with one another and in some categories – such as identity platforms – players have partnered with all the listed categories and more. While many of these partnerships make sense for the underlying businesses, they can cause problems for the enterprise (the customer). To explore this, consider the challenge that using more than one identity vendor poses to the consumer. How long does it take to enrol in a new service such as opening a bank account remotely? What consumer friction is involved? What are the headwinds to enrolment? How many steps will it take? Does the consumer feel safer, and does s/he understand the process? What about the enterprise back end? If the solution providers are cloud-based, how many API calls will the bank have to make potentially exposing customer data? What is the overall efficacy of the complete multi-assembled identity solution? What if four of the seven vendors say ‘yes’ (it is a verified you), but the other three say ‘no’? How can the bank properly orchestrate the identity results with confidence and configure the right algorithmic workflows? The questions and complications are nearly endless – and the list above does not even begin to consider the total cost of a multi-vendor solution.

Next-generation customer identity platform (CIP)

These questions appear ripe for a solution that enables frictionless identity and offers the required privacy protections, data management and compliance capabilities, custodial ownership, high efficacy rates, and seamless future portability of an individual’s identity.

I believe the winning solutions will enable both frictionless identity verification and reauthentication in a single, integrated platform. They will further allow for the use of multiple forms of proprietary and complementary authenticators and offer an intelligent real-time decision engine built on an automated, microservices and API-based cloud platform – all supported by an AI-based infrastructure with integrated enterprise tools and capabilities to optimise the consumer and employee experience.

In short, the future of identity is moving rapidly towards an integrated identity solution that can actively address critical questions such as ‘are you who you say you are?’, ‘what do you have?’, ‘what do you know?’, ‘where are you going in a session?’, ‘why – and most importantly – is this your predictive or past behaviour?’. AI-based intelligent verification and authentication is coming.

The content herein reflects the views of Ralph A. Rodriguez, Executive-in-Residence at Summit Partners, and is intended for entrepreneurs considering partnering with Summit Partners.

About Summit Partners: Founded in 1984, Summit Partners is a global alternative investment firm that is currently managing more than USD 21 billion in capital dedicated to growth equity, fixed income, and public equity opportunities. Summit invests across growth sectors of the economy and has invested in more than 500 companies in technology, healthcare, consumer, financial, and business services, and other growth industries. Summit maintains offices in North America and Europe, and invests in companies around the world. For more information, please see www.summitpartners.com or follow on [LinkedIn](#).

www.summitpartners.com



Overview of Key Industry Players

Mergers & Acquisitions in the Fraud Prevention Space – the Last 12 Months Overview



About Simona Negru: A graduate of English Language and Literature studies, with an MA in American Studies, Simona is always on the lookout for the best and new stories to capture. A passionate content editor, Simona is keen on discovering and sharing all the relevant topics on payments and commerce, as well as online security and digital identity, all while finding the hottest trends in the industry for The Paypers' readers.

Simona Negru ■ Content Editor ■ The Paypers

In order to keep up with all the changes and challenges in the industry that made their presence felt in the last 12 months, and to satisfy the need to stay above both competitors and fraudsters, some industry players have partnered, collaborated, invested in others, merged or acquired other businesses.

However, to have a better overview of the main deals and the reasons behind them, we have decided to depict some of the most significant mergers and acquisitions in the fraud space, in the last 12 months. In this M&A article, we discerned between companies that focus on **solutions aimed to secure digital transactions** (e.g. fraud prevention platforms) and companies that focus on **financial services and regulated entities that need to rely on KYC, identity, and compliance** mechanisms to prevent fraud and other types of system abuse.

The context

The current pandemic situation has proven to be challenging for many players operating in the payments industry. We see a growing number of online transactions, as lots of people have been forced to make a shift towards more and more digital channels in a bid to maintain social distancing and avoid contact. The lockdown forced people to carry out their daily banking and shopping activities online, while businesses that were new to the online channel, such as the case of many brick and mortar merchants, had to accommodate to the new normal. On the consumer side, this move to the digital world brought along a new vulnerable group of users, including the elderly who need to learn how to transact online; **minors engaging in remote learning; and subscribers looking to access online entertainment and streaming services**. Fraudsters may attempt to lure these less tech-savvy consumers into criminal activities or steal their identities in a bid to use them on fraudulent ventures.

What is more, criminal groups take advantage of the chaos provoked by the pandemic. As there are more transactions, the number of online fraudulent acts is also growing because not only fraudsters get access to online channels easily, but they are also opportunistic and come up with new different methods to do their jobs. Therefore, online fraud is on the rise, fraud has become increasingly sophisticated, and scammers continue to innovate new ways to defraud honest businesses.

Fraudsters seem to have all the tools that facilitate their work, especially now, and they do not hold back. They constantly elevate their game with advanced tools and go directly for merchant's accounts with complex account takeover (ATO) attacks; they use strategies like synthetic identity fraud, SIM card swaps; they gather personal information, credentials, and credit card numbers which they then use on the dark web.

At the same time, financial institutions face some issues as well – lots of people have remained without a job either because their **employer closed or lost the business due to the coronavirus pandemic**. KPMG reports that, during this period, companies around the globe apply for **emergency loans or government-backed support**, which makes them a target for fraudsters. →

Mergers & Acquisitions in the Fraud Prevention Space – the Last 12 Months Overview

Bad actors do not lose any opportunity for illicit activities: they pose as legitimate businesses or individuals seeking for financial assistance, so they use information in the public domain to make fraudulent claims on government schemes. There are also fraud and credit risks associated with the **bounce back loan scheme (BBLs)** – a new scheme designed to enable businesses to access finance more quickly during the coronavirus outbreak. The head of the British Business Bank emphasised upon the extensive reliance on customer self-certification and the corresponding fraud risk as being a key concern, and considered that the scheme is ‘vulnerable to abuse’ by participants in organised crime.

In addition, for those banks that had to close their branches, the online channel became the go-to channel. However, those that don’t have a well-developed online channel are at risk, because bad actors **circumvent controls to introduce illicit proceeds into the financial system**. So, activity supervisors and compliance teams need to re-assess what is unusual or suspicious. Some are forced to work remotely, so they no longer conduct on-site investigations, but they are reduced to desktop analysis, while others even employ online verification and authentication tools that they’re not familiar with. As such, since fraudsters will try to pose as legitimate individuals or businesses, or try to infiltrate financial systems, it is crucial for businesses to invest in digital onboarding and identity verification mechanisms to prevent fraud and money laundering.

In addition, KPMG reported that there has been noticed **an increase in phishing emails and in call centre fraud**. In the first case, the emails received may seem to come from banks, but they are either a lure asking for customers’ account information or a malware that downloads onto one’s system when the link is clicked. In call centre fraud, bad actors engage in social engineering, asking questions on social media platforms to obtain information that is further used to impersonate legit customers with their bank or to make a false insurance claim.

So, fraudsters perfect and scale their operations; but businesses need to uplift their defences as well as to respond to these threats correctly. The growing number of sophisticated attacks are forcing companies to invest in their security services, and to search for specific solutions to meet the challenges. Moreover, businesses are required to stay compliant with the new upcoming regulations (PSD2, SCA), and avoid any types of fines or reputational risk. This also drives the need to add more capabilities. As they are pushed towards implementing solutions that offer SCA, solution providers need to come into help.

This wider acceptance of digital processes and online transactions translates into the need for more tailored and safer services to a wider range of people. At the same time, safer services mean better tools to prevent fraudsters from abusing financial systems and compromising the KYC/AML checks. How can this be achieved? By investing in robust data-led solutions that are meant to manage fraud, identity, and compliance risks. LexisNexis reports that **‘in an increasingly digital world, data is king’**, therefore, it is important now more than ever to rely on KYC, identity, and compliance tools that are designed to detect and prevent bad actors from abusing the system.

Fraud prevention and detection: a shield to keep fraudsters at bay

The second half of 2019 started with a boom in terms of new innovations and acquisitions. F5 Networks, a US-based company that specialises in application services and application delivery networking (ADN), acquired Shape Security, a company that offers a fraud prevention platform to banks, airlines, retailers, government agencies, and more. The company also provides sophisticated bots, fraud, and abuse defences, and it specialises in protecting against credential stuffing attacks. As F5 wanted to better protect applications across multi-cloud environments, the company’s decision to acquire Shape Security was inevitable. The deal was agreed at USD 1 billion. →

Mergers & Acquisitions in the Fraud Prevention Space – the Last 12 Months Overview

In August 2019, Razorpay, an India-based paytech/fintech company, acquired NCR-based AI company Thirdwatch. Thirdwatch designed an AI platform to prevent real-time fraud in ecommerce companies, which led Razorpay to this strategic deal, as it wanted to increase its efforts at both improving payment experience and avoiding fraudulent transactions with the help of AI, ML, and Big Data.

Data and advanced analytics company LexisNexis Risk Solutions acquired a number of companies to obtain new fraud detection and risk assessment capabilities, as well as to **augment organic growth**.

In 2018, its parent company, RELX Group, closed the acquisition of ThreatMetrix for **USD 817 million in cash**, in a bid to allow companies around the world to protect themselves against existing and emerging fraud, risks, and financial crime with new innovative solutions; and to enable a comprehensive approach to fraud and identity risk management.

In January 2020, LexisNexis agreed to purchase NortonLifeLock's ID Analytics, a deal that is expected to close in Q1 2021 for USD 375 million. The aim is to help with the delivery of risk insight via a combination of proprietary data, patented analytics, and near-real-time cross-industry consumer identity behaviour.

In March 2020, LexisNexis acquired Emailage, a fraud prevention and risk management solution provider that operates in this space. As now part of the Business Services group of LexisNexis Risk Solutions, Emailage's email and digital data attributes network, inquiry data, and confirmed fraud feedback will complement LexisNexis' **expertise in contributory data management and linking technology**.

LANDRY et associés, a multidisciplinary firm specialising in risk and performance management, grasped the opportunity to expand into the Canadian market. This was possible with the completion of NexuWeb's acquisition – an ecommerce security and development services company. NexuWeb offers anti-fraud services and it has an expertise in credit card bank fraud and cryptos. LANDRY benefits from the opportunity **'to become a leader in the Canadian market in fraud prevention and protection of cryptocurrency transactions'**, as well as from an array of ecommerce services, such as infrastructure security, content delivery acceleration, and fraud prevention and cryptocurrencies.

In June 2020, the payments testing and consultancy company FIME unveiled the acquisition of CETECOM US's payment activities. CETECOM is an independent test and certification service provider. What FIME did through this move is actually enabling the US payment ecosystem to define, design, deliver, and test new digital payments products. Both teams will work together to support the acceleration of digital payment technologies in the US, from authentication solutions around biometrics and EMV 3DS, through to card, mobile, and softPOS contactless payments.

Identity authentication platform Prove (formerly Payfone) – a customer identity platform that provides mobile and digital identity authentication solutions for businesses – unveiled the acquisition of mobile authentication lines of business from Early Warning Services – a fintech company owned by seven of US largest banks, whose goal is to empower financial institutions to make confident decisions, enable payments, and mitigate fraud. This move continues an initial partnership started in 2013, agreed upon the delivery of authentication solutions to the US financial services industry. As per Prove's CEO, the acquisition will accelerate the **'growth and penetration into financial institutions around the globe, positioning Prove as the global standard for customer identity and authentication'**. →

Mergers & Acquisitions in the Fraud Prevention Space – the Last 12 Months Overview

A glimpse into a world of identity, KYC, and financial crime compliance

Moody's Analytics, a unit of Moody's Corporation, which helps capital markets and credit risk management professionals, acquired risk analytic solution company RiskFirst. This move proves profitable for Moody's because RiskFirst's platform addresses the US and UK defined benefit pension markets, offering solutions for the institutional investment market. With this acquisition, Moody's extends its range of risk solutions to the institutional buy-side.

The spring of 2020 also brought new deals. Acuant, a provider of identity verification solutions across the global market, finished the acquisition of its strategic partner IdentityMind. This means that Acuant's Trusted Identity Platform for identity proofing and verification is currently combined with IdentityMind's Digital Identity Platform for identity creation, risk scoring, transaction monitoring, and regulatory compliance (KYC and AML). By merging these two platforms, Acuant's newly evolved identity platform will now provide building, proofing, verifying, and maintaining digital identity services, making it a complete identity management solutions package.

In September this year, identity verification platform IDnow revealed the decision to sign an agreement for the acquisition of Wirecard Communication Services, which is part of the Wirecard Group. The acquisition has various objectives: first, to facilitate the service quality of IDnow products; second, to further increase the responsiveness for customers; and third, to cut waiting times.

NICE Actimize, a provider of financial crime, risk, and compliance solutions, acquired Guardian Analytics, an AI cloud-based financial crime risk management solution provider. By combining both companies' fraud and AML capabilities, they believe businesses will be empowered to adopt solutions that best protect their assets and customers. NICE wanted **'to make sure financial institutions and consumers are protected in a way that's cost-effective and intuitive.'** The plan is to offer AML and fraud capabilities in the cloud for financial crime and compliance coverage, analytics and ML solutions that adapt to new attacks and allow higher detection, lower false positives, and a 360-degree view for operational efficiency.

Regulatory DataCorp (RDC), a risk intelligence company and a provider of AML and KYC data and due diligence services, was acquired by Moody's Corporation. This agreement is meant to complement Moody's 2017 acquisition of company data provider Bureau van Dijk (BvD) **by deepening its information portfolio and analytical capabilities** through the addition of RDC's comprehensive dataset. The deal extends RDC's global presence to a broader group of financial institutions, corporations, insurance companies, and government agencies served by Moody's Analytics and BvD.

Accuity, a global provider of financial crime screening, payments, and KYC solutions, and part of RELX, announced the acquisition of Apply Financial Limited (Apply Financial), which offers payments validation solutions to both financial institutions and corporates using the cloud and API's. Via this deal, Accuity supports its strategy of providing banks, corporates, non-banking financial institutions (NBFIs), and fintechs with global and domestic payment and account validation solutions that reduce payment processing costs while increasing the speed of transactions. Apply Financial believes that they **'will be able to share industry expertise, [...], and collaborate on innovative solutions that will support the industry now and in the future.'**

Refinitiv, a provider of financial markets data and infrastructure, signed an agreement to acquire digital identity, payments verification, and fraud prevention company GIACT. Via the addition of GIACT's fraud prevention capabilities, Refinitiv broadens its digital identity verification and document proofing solution, dubbed Qual-ID. GIACT reports that together, both companies, **'will bring to market a unique platform that can address the complete customer lifecycle, regardless of industry'**. Thus, customers will also be offered an end-to-end fraud prevention, identity verification, and compliance platform that addresses money-laundering risks in addition to preventing monetary loss through fraud. →

Mergers & Acquisitions in the Fraud Prevention Space – the Last 12 Months Overview

Final notes

If we are to look into the future and consider some trends that most likely will be seen in 2021, what exactly can we see?

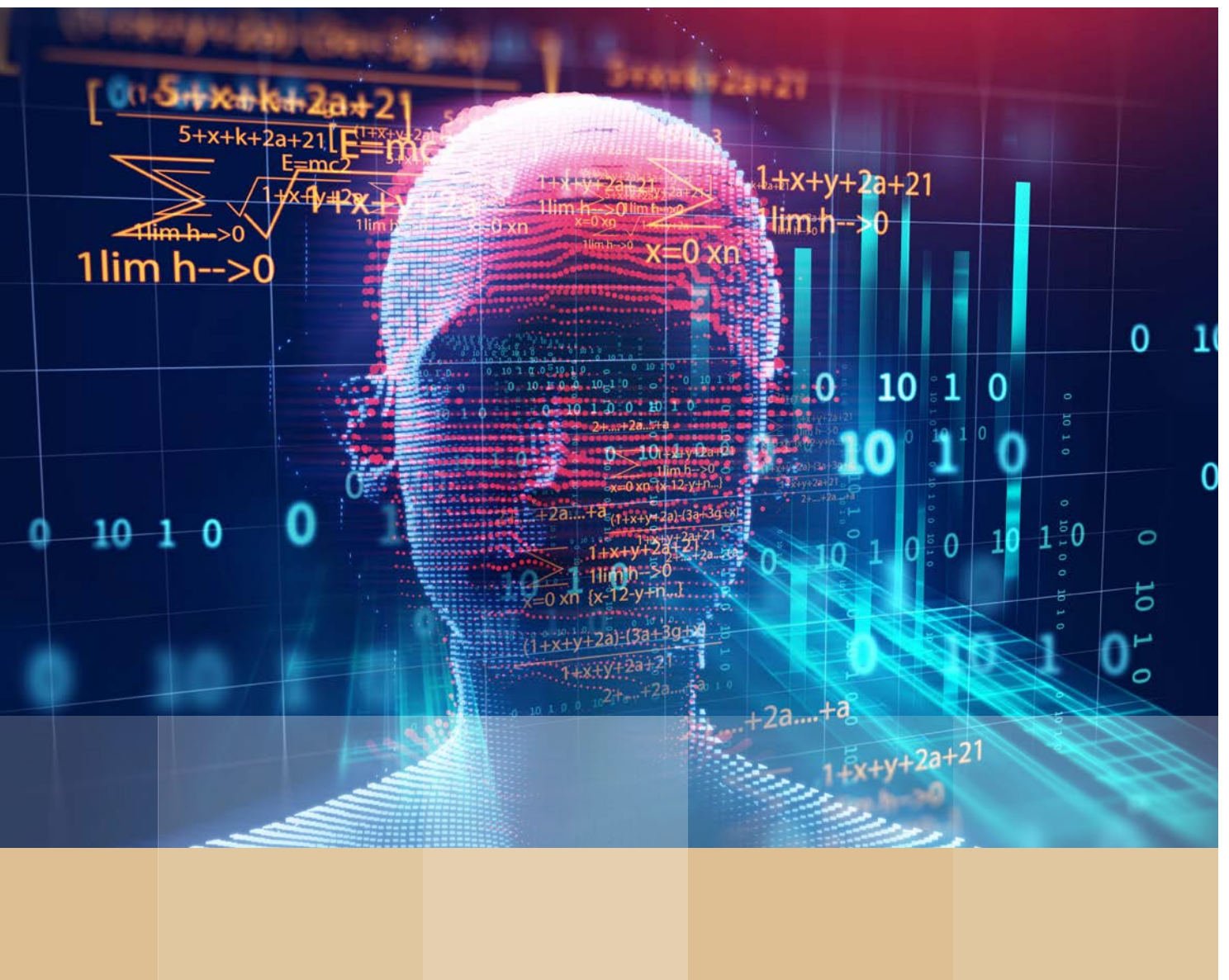
Well, firstly, we can see without a doubt the impact of the global lockdown that has changed everyone's lifestyle. Not only has the pandemic accelerated the move towards digital channels, but consumers have had to adapt to new ways of shopping, while merchants have had to reconsider their payments and delivery infrastructure. Many businesses started to collaborate with more and more delivery companies to provide customers with their bare necessities and to meet their expectations and conveniences.

This means that companies will continue to invest in state-of-the-art tools to protect their good customers and block bad actors. Solution providers will invest in and acquire more capabilities to widen their datasets and improve their data analytics features. The tricky part, however, is that fraudsters will watch everything, and they will also want to create more sophisticated tools to outsmart solution providers. Therefore, to stay one step ahead of fraudsters, we will likely see more acquisitions in 2021: just as LexisNexis did, for instance – businesses will collaborate to increase and leverage their datasets and offer advanced analytics.

Secondly, COVID-19 has also accelerated the rate of digital adoption in financial services. This will not stop here either. The move towards a digital economy implies one's trust in the technology that is meant to provide a safe environment for transactions. This is why reliance on robust KYC and compliance tools to prevent money laundering and fraud is a must. Thus, companies will continue to focus on financial services and regulated entities that need to rely on identity tools. Also, let's consider one more important thing that will change the game for all players: the new upcoming regulation (PSD2) that raises the compliance questions – Who will be ready? Who will have the best compliant suits?

In addition, biometric payment cards, for instance, are expected to become a huge trend **towards the use of multi-factor contactless transactions** in the aftermath of the pandemic. The reason for this is the fact that COVID-19 has already driven a significant shift in consumer spending habits, and there is a visible surge in ecommerce. At the same time, governments bodies are urging consumers to limit the use of cash in favour of digital payment methods. This does not mean that the concerns about fraud will diminish, but biometric cards, which require a fingerprint scan on a card, are expected **to make fraud more difficult, as criminals would have to create a synthetic print**. The question here is: who will embark on the journey of creating these preventive solutions? And most importantly, who will partner, merge or drive these acquisitions? With one step closer to 2021, we should only wait and see what's coming next.

Simona Negru | Content Editor | The Paypers



Solution Providers – Mapping of
Core Features and Capabilities

Introduction

Fraud attacks are steady in 2020, in part due to the COVID-19 pandemic that created vulnerabilities at all levels, and emerging fraud trends are making their way across the payments industry. From preventing omnichannel fraud, account takeover, friendly fraud (on the rise) to implementing PSD2 SCA, businesses have a hard mission to meet all these challenges. For this reason, businesses need state-of-the-art tools and technologies to accept more orders while reducing customer friction and false positives to protect their customers and increase their revenue.

In order to find the right partner to join forces with in this never-ending fight against fraud, businesses need to understand the new technologies and features that are developed relatively at a rapid pace, and learn about the vendors that offer them. So, we have put together a comprehensive mapping of solution providers that displays their services ranging from decisioning platform, identity verification, authentication, data intelligence, chargebacks management to spam and abuse, and bot management.

Upgraded features and technologies to fight fraud

Either old or emerging, fraud trends cover all commerce verticals, perhaps some of them more than the others, but every aspect revolves around (new) account fraud and card-not-present (CNP) fraud now. Fraudsters are taking advantage of the loopholes, especially now, that ecommerce surged at a too rapid pace and businesses must handle an unprecedented volume of online orders.

With an increased level of fraud complexity, traditional solutions (such as rule-based only) and siloed processes (siloed), are no longer enough on a fraud management agenda. To keep the pace with the sophisticated attacks, solution providers must level up their products to support the players operating in the commerce space – from merchants to PSPs, acquirers, and fintechs – to fight fraud in an effective manner.

The **AI-driven** technologies have been augmented with various features that leverage machine learning, behavioural analytics, biometrics, data enrichment, and bot detection tools. Real-time transactions rely heavily on real-time detection tools – automated and smart solutions that can prevent false positives.

Merchants should look to incorporate new technologies that create frictionless barriers and a hard life for fraudsters to operate, while improving acceptance rates. **Behavioural analytics** and **biometrics** are a good way to identify a bad actor without affecting the customer experience. In order to fight account takeover, for instance, a powerful combination is behavioural analytics, behavioural biometrics, and **device intelligence** for improved risk-based decisions, especially in contextual commerce. As we see that new fraud types emerge, it's key to also establish the behavioural patterns that emerge from the customer journey. For more informed decisions, higher quality data is also needed, so **data enrichment** plays an important role here, to better learn the modus operandi of fraudsters. Moreover, to outsmart fake impersonators aka bad bots and their lifecycle, a strong **identity verification solution** is needed, which once again relies on features such as behavioural analytics, device-based data, transactional data, and risk-based analysis, all invisible for the end-consumers. Relevant companies using these strategies are Arkose Labs, Fraugster, SecuredTouch, Seon, to name a few.

Machine learning is here to stay – there is a relatively common message that supervised and unsupervised ML should be employed, leaving enough room for human intelligence to train the algorithms. The combination of knowledge-based methods and ML driven models are now part of a good risk management strategy. And this is where **explainable AI** comes in, having the role to extract knowledge from a detection model and to explain how the machine made specific decisions. So taking into account supervised and unsupervised machine learning, explainable AI, and human intelligence, it's fair to say that a hybrid AI approach is the best to go with. We recognise as companies applying advanced ML techniques Kount, Sift, and Simility. →

Introduction

PSD2's SCA as a separate challenge





The demand for secure and frictionless customer experience prompts solution providers to improve their existing authentication methods. Ecommerce businesses, on the other hand, must collaborate with compliant fraud prevention solutions to conduct SCA and keep control of their rates, and this is possible with EMVCo's 3DS protocols-based services. 3-D Secure is an authentication tool, currently deployed by the card schemes (via Visa Secure, Mastercard Identity Check, American Express SafeKey, or Discover ProtectBuy), being a secure way to verify ecommerce transactions. However, the need for more security and convenience on the customer side asked for a new version: **3-D Secure 2.0**. A smooth transition to 3-D Secure 2.0 implies great support from PSPs or/and vendors – they have to help merchants checking the technical documentation for payment gateway integration, implementing transaction flows, initiating data collection, and on top of all, making sure that SCA enforcement timelines are met. Basically, implementing a seamless SCA is a journey that merchants and their solution providers must take together.

FIDO2 authentication protocol, developed by FIDO Alliance, is another option to deploy for a frictionless omnichannel experience, so merchants should also keep an eye on companies that have FIDO authentication integrated into their solutions. FIDO standards-based strong authentication combines cryptographic protection of user authentication credentials and biometric data, that never leaves the user's device. Moreover, FIDO authentication might be used as input to 3-D Secure processes. Several companies offering solutions such as 3-D Secure 2.0 and SCA compliant authentications are Cybersource, Entersekt, Kount Nok Nok Labs, Netcetera, Signifyd.





There is a plethora of solution providers across the industry, but which one is best suited for your needs? Check out our overview of fraud and risk management solution providers to see who can back up your system with anti-fraud tools and help you in creating a tailored anti-fraud strategy.

Anda Kania | Senior Editor | The Paypers





Solution Providers – Mapping of Core Features and Capabilities

Company Name				
Background information				
Year founded	2016	2008	1975	2016
Target group				
Banks/FS	X	X		X
Corporate	X	X	X	X
Fintech	X	X	X	X
Merchants/ecommerce	X	X	X	X
PSP/acquirers	X	X	X	X
SMBs		X	X	X
Telecom			X	X
Supported Regions	Global	North America, LATAM, APAC, EMEA	US, Europe, Middle East, APAC, Africa, LATAM	Global
Core solution				
Company description	4Stop provides access to hundreds of premium global KYB and KYC data services combined with their compliance and automated, real-time and dynamic anti-fraud technology with advanced monitoring intelligence and data science.	Leading provider of fraud prevention, chargeback management, digital identity, and payment gateway solutions. Accertify's layered risk platform, machine learning backbone, and rich reputational community database enables businesses to address challenges across the entire customer journey.	Multi-layered online and mobile fraud detection and prevention, with an emphasis on increasing conversion while reducing fraud and chargebacks	Arkose Labs bankrupts the business model of fraud. Recognised by Gartner as a 2020 Cool Vendor, its innovative approach determines true user intent and remediates attacks in real time. Risk assessments combined with interactive authentication challenges undermine the ROI behind attacks, providing long-term protection while improving good customer throughput.
Fraud and risk management	X	X	X	X
Decisioning platform	X	X	X	X
Identity verification	X	X	X	
Authentication	X	X	X	X
Data provider and Intelligence	X	X		X
Chargebacks management		X	X	
Spam and abuse	X	X		X
Bot Risk Management	X	X		X
Technology				
On-premises	X	X		
Cloud enabled	X	X		
Native cloud			X	X
Hybrid		X		
P = proprietary capability, T = third party, P/T = proprietary capability/third party				




Solution Providers – Mapping of Core Features and Capabilities

Company Name				
Data Input				
Identity Verification				
Identity Document Scanning	T			
Video scanning	T			
Personally Identifiable Information (PII) Validation	T	P/T	P	
Small Transaction verification	P		P	
Email verification	T	P/T	T	
Phone verification	T	T	T	
Social verification		T	T	
Credit check	T			
Compliance check	T	T		
Online Authentication				
Behavioural biometrics	P	P	P	P
Physical biometrics	T		P	
Device fingerprinting	P/T	P	T	P
Geo-location	T	P	T	P
Remote access detection	T	P	T	
Mobile app push	T	P	P	
3-D Secure 2.0		T	P	
Hardware token	T		P	
One-time passwords	T	T		
Knowledge-Based Authentication	T	T	P	
Intelligence				
Abuse list	P/T	P	T	P
Monitoring	P/T	P	P	P
Address Verification	T	T	P/T	
Credit Bureau	T	T		
Information Sharing	P	P	P	P
Data Ingestion/Third Party Data				
Stateless Data Ingestion and Augmentation	X	X	X	
P = proprietary capability, T = third party, P/T = proprietary capability/third party				





Solution Providers – Mapping of Core Features and Capabilities

Company Name				
Methodology				
Machine Learning				
Rule-Based	X	X	X	
Supervised ML	X	X	X	X
Unsupervised ML			X	
Hybrid		X	X	
Decisioning				
Manual review	X	X	X	
Case management	X	X	X	
Decision orchestration	X	X	X	X
Chargeback Management				
Chargeback dispute	X	X	X	
Guaranteed fraud protection	X	X	X	
Business Model				
Pricing				
Pricing model	Pricing is per 'Core Service' and/or 'Verification KYC' transaction and based on volume and complexity.	Confidential	Pricing is per transaction and based on volume and complexity OR SaaS-based pricing model.	SaaS pricing
Services				
Managed Service	X	X	X	X
Training & Support	X	X	X	
Customers				
Customer Reference	Mifinity, Draglet, Gatehub, Paysend, Paymentz, eMerchantPay, Paytah by Monetum, BCCS, Hexopay	Provided upon request	Aegean Airlines, Amadeus, Crew Clothing, EE, HyperPay, John Lewis, Mango	Microsoft, EA
P = proprietary capability, T = third party, P/T = proprietary capability/third party				




Solution Providers – Mapping of Core Features and Capabilities

Company Name	 COVERY SOLVE FRAUD	CyberSource® A Visa Solution	 Entersekt	 Fraugster
Background information				
Year founded	2016	1994	2008	2014
Target group				
Banks/FS	X	X	X	
Corporate	X	X		X
Fintech	X	X	X	X
Merchants/ecommerce	X	X	X	X
PSP/acquirers	X	X	X	X
SMBs	X	X		X
Telecom		X		
Supported Regions	Global	Global	Africa, Europe, LATAM, Middle East, North America	Global
Core solution				
Company description	KYC/KYB automation, charge-back mitigation, ALM screening; affiliate, friendly, credit card, CNP, payment fraud, account take-overs, and identity theft prevention	With Cybersource's global fraud management platform merchants and acquirers can reduce fraud, increase agility and improve the customer experience. We do this by bringing customers more insights, more options and a more complete approach.	Entersekt is a leading provider of device identity and customer authentication solutions. Its multi-patented, regulatory compliant technology helps financial institutions and other enterprises to build trust and boost loyalty with secure, convenient, and engaging new digital experiences.	Fraugster is an AI-based payment security company, which helps online merchants maximise their revenues while simplifying operations. We help our clients reduce fraud and false positives and increase approval rate.
Fraud and risk management	X	X	X	X
Decisioning platform	X	X	X	X
Identity verification	X	X	X	
Authentication		X	X	
Data provider and Intelligence		X	X	
Chargebacks management	X			
Spam and abuse	X			
Bot Risk Management	X		X	X
Technology				
On-premises			X	
Cloud enabled	X	X	X	
Native cloud		X	X	X
Hybrid			X	
P = proprietary capability, T = third party, P/T = proprietary capability/third party				






Solution Providers – Mapping of Core Features and Capabilities

Company Name	 COVERY SOLVE FRAUD	 CyberSource® A Visa Solution	 Entersekt	 Fraugster
Data Input				
Identity Verification				
Identity Document Scanning	T		T	
Video scanning	T		T	
Personally Identifiable Information (PII) Validation	T	P	T	
Small Transaction verification		P		
Email verification		P		
Phone verification		P	P/T	
Social verification		P		
Credit check				
Compliance check				
Online Authentication				
Behavioural biometrics			P/T	
Physical biometrics			P/T	
Device fingerprinting	P	P	P/T	P
Geo-location	P	P	P	P
Remote access detection	P	P		P
Mobile app push			P	
3-D Secure 2.0		P	P	
Hardware token		P	P/T	
One-time passwords			P	
Knowledge-Based Authentication			P	
Intelligence				
Abuse list	P	P	P	
Monitoring	P	P		P
Address Verification		P		
Credit Bureau				
Information Sharing		P		P
Data Ingestion/Third Party Data				
Stateless Data Ingestion and Augmentation	X	X	X	X
P = proprietary capability, T = third party, P/T = proprietary capability/third party				






Solution Providers – Mapping of Core Features and Capabilities

Company Name	 COVERY SOLVE FRAUD	CyberSource® A Visa Solution	 Entersekt	 Fraugster
Methodology				
Machine Learning				
Rule-Based	X	X	X	
Supervised ML	X	X	X	X
Unsupervised ML		X	X	
Hybrid	X	X	X	X
Decisioning				
Manual review	X	X		X
Case management	X	X		X
Decision orchestration	X	X	X	X
Chargeback Management				
Chargeback dispute				
Guaranteed fraud protection				X
Business Model				
Pricing				
Pricing model	Various pricing plans for small and large businesses are available. Most of pricing plans are based on the volume of Decision API calls.	Tiered SaaS-based pricing model	Please email sales@entersekt.com for more information.	Fire Fixed price per transaction model, actual pricing depending on total processed transactions per month by the merchant. Additional product packages available covering expert analytics support or fully outsourced risk management service (covering all payment methods). FraudFree Pricing is based on a fixed percentage per transaction value. Pricing is dependent on the risk profile of the merchant, as Fraugster is taking over full liability for chargebacks from credit card transactions.
Services				
Managed Service	X	X	X	X
Training & Support	X	X	X	X
Customers				
Customer Reference	Genome, UniPay, Fastshift (Betconstruct), Mobeetech, Mr.Bet, Boosta, AskFm	Rue du Commerce (Decision Manager), ghd (Decision Manager), Cencosud / Paris.cl (Decision Manager), DICK'S Sporting Goods	Those listed in the public domain: Absa, Bayern Card-Services, Capitec Bank, Coutts, Discovery, Ecobank, Equifax, Equity Bank, FIS, FirstBank of Colorado, Investec, Nedbank, Old Mutual, Pluscard, Swisscard. For others, please email sales@entersekt.com	Ingenico ePayments, Six Worldline, Ratepay, Eurostep, AS Adventure, Diana SRL, European Games Group, Krefel
P = proprietary capability, T = third party, P/T = proprietary capability/third party				






Solution Providers – Mapping of Core Features and Capabilities

Company Name					
Background information					
Year founded	1990	2007	1996	2011	2014
Target group					
Banks/FS	X	X	X	X	X
Corporate	X	X			
Fintech	X	X	X	X	X
Merchants/ecommerce	X	X	X	X	X
PSP/acquirers	X	X	X	X	X
SMBs		X		X	
Telecom		X		X	
Supported Regions	Global	Global	Europe, Middle East, APAC, Africa, Americas	Global	US, Europe, Middle East, APAC, Africa, LATAM, India
Core solution					
Company description	ISoft's omnichannel risk management solutions are based on the fastest AI and behavioural analysis technology for threat detection in real-time and immediate response to new and known fraud patterns.	Kount's Identity Trust Global Network delivers real-time fraud prevention, account protection, bot detection, and enables personalised customer experiences for more than 9,000 leading brands and payment providers.	Netcetera is serving the issuers, acquirer, and network domains with advanced solutions to increase the conversion and to deliver an outstanding payment experience.	We help companies authenticate users so they can provide digital services in a simple, secure, and scalable experience. We deprecate passwords and accelerate cost-effective, future-proof, and standards-based authentication.	SecuredTouch provides visibility into the entire customer journey to uncover behavioural anomalies and non-human behaviours, and detect fraud at any stage, before checkout, even when no transaction takes place.
Fraud and risk management	X	X	X		X
Decisioning platform	X	X			
Identity verification	X	X	X	X	
Authentication	X		X	X	X
Data provider and Intelligence		X			
Chargebacks management		X			
Spam and abuse					
Bot Risk Management		X			X
Technology					
On-premises	X		X	X	
Cloud enabled	X	X	X	X	X
Native cloud	X	X	X		X
Hybrid	X			X	X
P = proprietary capability, T = third party, P/T = proprietary capability/third party					

Solution Providers – Mapping of Core Features and Capabilities





Company Name					
Data Input					
Identity Verification					
Identity Document Scanning	T			T	
Video scanning	T			T	
Personally Identifiable Information (PII) Validation	T	P			
Small Transaction verification	P	P			
Email verification	T	P		P	
Phone verification	T	T		P	
Social verification	T				
Credit check					
Compliance check					
Online Authentication					
Behavioural biometrics	T	P	T	T	P
Physical biometrics	T		P	P/T	
Device fingerprinting	T	P	P	P	P
Geo-location	T	P	P	P	
Remote access detection		P			
Mobile app push	T		P	P	
3-D Secure 2.0		P	P	P	
Hardware token			T	T	
One-time passwords			P	P	
Knowledge-Based Authentication			P		
Intelligence					
Abuse list	P	P			T
Monitoring	P	P			T
Address Verification	T	T			
Credit Bureau	T				
Information Sharing	P	P			
Data Ingestion/Third Party Data					
Stateless Data Ingestion and Augmentation	X	X	X	X	
P = proprietary capability, T = third party, P/T = proprietary capability/third party					

Solution Providers – Mapping of Core Features and Capabilities





Company Name					
Methodology					
Machine Learning					
Rule-Based	X	X	X		X
Supervised ML	X	X	X		X
Unsupervised ML	X	X	X		X
Hybrid	X	X	X		X
Decisioning					
Manual review	X	X			
Case management	X	X			
Decision orchestration	X	X			X
Chargeback Management					
Chargeback dispute		X			
Guaranteed fraud protection		X			
Business Model					
Pricing					
Pricing model	Information available upon request	Kount has different pricing models by use case and desired services.	Authentication as service, annual fee for on-premise	Per user annual subscription	Based on session volume
Services					
Managed Service	X	X	X	X	X
Training & Support	X	X	X	X	X
Customers					
Customer Reference	4 of the 10 largest European Banks equipped, and more than EUR 40 billion protected every day	Kount protects 9,000+ customers globally, including Staples, Dunkin, AMC, Intuit, BP, Telstra, and more. kount.com/customers	More than 2000 issuers rely on Netcetera 3DS and authentication services; 60,000+ merchants worldwide use 3DS acquiring services and products from Netcetera.	NTT DOCOMO, T-Mobile, BBVA, Intuit, Standard Bank, MUFG, and more	Trusted by top global merchants, including Wish.com, Gett & MIT.

P = proprietary capability, T = third party, P/T = proprietary capability/third party

Solution Providers – Mapping of Core Features and Capabilities

Company Name				
Background information				
Year founded	2017	2011	2011	2014
Target group				
Banks/FS	x			x
Corporate	x	x		
Fintech	x	x		x
Merchants/ecommerce	x	x	x	x
PSP/acquirers	x	x		x
SMBs	x	x		
Telecom	x			
Supported Regions	Global	US, EMEA, APAC, LatAM, Australia/ New Zealand	Global	US, Europe, AsiaPac, India, China, LATAM, Africa, Middle East
Core solution				
Company description	SEON reduces the costs, time and resources lost to fraud. SEON is designed around two core goals: deliver effective risk prevention, and give businesses complete freedom in how they fight fraud.	Sift, the leader in Digital Trust & Safety, empowers companies to unlock revenue without risk and prevent fraud with industry-leading technology and an unrivaled global data network.	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.	Similarity's Adaptive Decisioning Platform leverages advanced machine learning to dynamically decision across a wide variety of use cases, including new account origination, account takeover, and transaction fraud.
Fraud and risk management	x	x	x	x
Decisioning platform	x	x	x	x
Identity verification	x		x	x
Authentication			x	
Data provider and Intelligence	x		x	
Chargebacks management	x		x	
Spam and abuse	x	x	x	
Bot Risk Management	x		x	
Technology				
On-premises	x			x
Cloud enabled	x	x		x
Native cloud	x	x	x	
Hybrid	x			x
P = proprietary capability, T = third party, P/T = proprietary capability/third party				

Solution Providers – Mapping of Core Features and Capabilities

Company Name				
Data Input				
Identity Verification				
Identity Document Scanning		T		
Video scanning				
Personally Identifiable Information (PII) Validation		T	P	T
Small Transaction verification			P	
Email verification	P	P/T	P	T
Phone verification	P	T	P	T
Social verification	P		P	T
Credit check				T
Compliance check			P	
Online Authentication				
Behavioural biometrics			P	T
Physical biometrics				
Device fingerprinting	P	P	P	P
Geo-location	P	P	P	T
Remote access detection	P	P	P	T
Mobile app push		T	P	
3-D Secure 2.0		T	P	
Hardware token			P	
One-time passwords		P	P	
Knowledge-Based Authentication				
Intelligence				
Abuse list		P	P	P
Monitoring		P	P	P
Address Verification		T	P	T
Credit Bureau				T
Information Sharing	P	P	P	P
Data Ingestion/Third Party Data				
Stateless Data Ingestion and Augmentation	x	x	x	x
P = proprietary capability, T = third party, P/T = proprietary capability/third party				

Solution Providers – Mapping of Core Features and Capabilities

Company Name				
Methodology				
Machine Learning				
Rule-Based	x	x	x	x
Supervised ML	x	x	x	x
Unsupervised ML		x	x	x
Hybrid	x	x	x	
Decisioning				
Manual review	x	x		x
Case management	x	x	x	x
Decision orchestration	x	x	x	x
Chargeback Management				
Chargeback dispute			x	
Guaranteed fraud protection			x	
Business Model				
Pricing				
Pricing model	Pure api, no setup, no support, and free trial	Volume-based	Various models	Transaction based, dependent upon use case
Services				
Managed Service			x	x
Training & Support	x	x	x	x
Customers				
Customer Reference	https://seon.io/references/	Airbnb, Boltpay, Box, Cabify, Carousell, ChowNow, Destinia, Doordash, Everlane, Fitbit, GetYourGuide, Glassdoor, Harry's, HelloFresh, Hopper, Indeed, Instacoins, Kamernet, Logitravel, Patreon, Poshmark, Pushpay, Rapyd, Reddit, Ritual, SendCloud, Shutterstock, Startselect, Traveloka, Turo, Twilio, Twitter, Unity, Upwork, Viagogo, Wayfair, Yelp, Zillow	Emma Mattress, Lacoste, Illy, Lego, Samsung, Mango, Omega, Reckitt Benckiser	Public references include US Bank, Jumia, OfferUp, Zions Bank
P = proprietary capability, T = third party, P/T = proprietary capability/third party				



The Impact of SCA Implementation – Now and After

In the light of the upcoming PSD2's Strong Customer Authentication deadline, merchants, fintechs, PSPs, and issuers must comply with the regulation. However, many businesses are still not ready for the new changes and require either exemptions or delays for the deadline. In this chapter, we will see which authentication methods need to be implemented to be compliant, secure, and frictionless, what more we need to know about 3-D Secure 2.0 and the future of SCA, as well as insights regarding security aspects after SCA implementation.

MRC Advocates Extension as SCA Enforcement Deadline Approaches



About Julie Ferguson: Julie Ferguson, the newly appointed CEO, has 25+ years of experience in developing, delivering, and promoting Internet-based technologies. She generates collaborations around industry problems and is enthusiastic about new technologies. Julie has a proven track record of bringing key stakeholders together to solve major problems and positioning existing technology to meet the needs of the audience, without changing fundamental value, proving to be a resourceful problem solver.

Julie Ferguson ■ CEO ■ MRC



About Úna Dillon: Úna is a regular public speaker on payments and has chaired working groups for organisations including the EPC. She ran Laser Card, the Irish debit card scheme, for 12 years, and was Head of IPSO Card Services, responsible for driving the development of policy on major initiatives such as SEPA.

Úna Dillon ■ Managing Director ■ MRC

MRC and our members are excited about the promise of SCA and EMV® 3-D Secure (EMV 3DS). Improved security for consumers, fewer fraudulent transactions, and increased authorisation rates are what we all want. Prior to the COVID-19 pandemic, the industry made progress to hit the European Banking Authority (EBA) enforcement deadline. Unfortunately, between the pandemic and the economic downturn, we believe the industry will not be ready by the current deadline of 31 December 2020.

In May, we began talking to merchants and issuers about their readiness concerns and sent **letters to the EBA** and to the **European Commission (EC)** to reflect real concerns. We also co-signed an industry letter from the **European Payment Institutions Federation (EPIF)** to the EC and EBA.

As we spoke with members about the challenges of EMV 3DS, one of our card issuing members shared that with significant growth in ecommerce caused by COVID-19, many new merchants are pivoting from card present sales to ecommerce transactions and there have been notable speed bumps. They shared one story that really drove

home the issue, specifically where a consumer placed an order for groceries for curbside pickup, the transaction failed on the day of pickup and the consumer was unable to collect their groceries. We need to remember, as we look at the data, each decline of a good consumer is not just a statistic, but a person who needs goods or services during a global pandemic.

The EC replied stating the deadline would not be moving. Two of our merchant members, Microsoft and Amazon, have created EMV 3DS implementation scorecards for the EU region that show, by country, the acceptance rates as well as many other key metrics. We provided these scorecards to the EBA, EC as well as to many National Conduct Authorities (NCAs). Scorecards can be requested from the **MRC**.

Microsoft published their methodology on creating the scorecard and we can now facilitate briefings for regulators and issuers to view monthly country scorecards for Microsoft, Amazon, Google, and Sony Interactive Entertainment. →

Measuring the impact of enforcing EMV 3DS and understanding the consumer impact is critical. Data tells the real story, and 4 major merchants, Amazon, Microsoft, Sony Interactive Entertainment, and Google data tell similar stories; the industry is not ready with EMV 3DS implementation. The consumer will suffer when they can't purchase online.

There are three main areas of concern around enforcement from the current deadline:

1. While implementation has been improving, there are still fundamental failures in the system. Based on current dashboards from a few merchant members in several countries, such as France, Belgium, and Italy, we would predict that 1 out of every 4 authentication attempts would fail.
2. While orders placed through a web browser are seeing reasonable performance in several countries, orders through mobile applications or game consoles in most countries still simply do not work, as many issuers are relying on falling back to 3DS 1.x which is not designed to work with mobile apps and consoles.
3. The deadline is at a very bad moment for merchants and issuers – in addition to the global pandemic slowing things down as volumes have more than doubled for many ecommerce merchants and issuers and the technology focus has been on scaling, it is also important to note that most issuers and merchants have code freezes between 21 November and 15 January, during the holiday peak season; so if something isn't working, bugs are identified, and the industry at large will have to wait post the holiday season to implement the changes.

All these merchants measuring EMV 3DS as part of their implementation proceed with an authorisation even if 3DS authentication fails.

With data in hand, the MRC began a virtual roadshow with merchant members, to the regulators in each country (NCAs), which are responsible for enforcing the regulation. To date, the MRC has facilitated 18 meetings. In some countries, we have been one of the many voices advocating for concessions and we are relieved to see the deadline shifting. The MRC is coordinating with our merchant community, working with the NCAs and we have published a **collaborative calendar** of the country deadlines on our website for our merchant members to stay current of the changes.

MRC also heard from issuers and merchants that it is extremely hard to test and debug problems, so we established a Slack channel, where the community is working together to solve these problems. To sign up for testing with Visa, email them at GCT3DSSUPP@visa.com. To sign up for the Mastercard test platform, [visit this page](#).

We are educating our members and encouraging them to use the testing platforms **Visa** and **Mastercard** have provided. We are fans of SCA and EMV 3DS, and as we review the data today, you will see a lot of great progress. In fact, the UK is a clear leader in the rollout of EMV 3DS and we are pleased that even with the progress being made, the UK recognised the potential risks of implementing the deadlines too early and the UK is the first country to push the deadline to September 2021. Other European countries have now moved their deadlines as well, such as France and Denmark.

We request that other countries take similar approaches and at the MRC we are ready to work with our members to pull together merchant data for any country or issuer who wishes to benchmark and assess their readiness.

About MRC: The MRC is a global membership organisation connecting ecommerce fraud and payments professionals through educational programmes, online forums, career development, conferences, and networking events. The MRC encompasses a membership network of over 500 companies including 350+ merchants all focused on fraud prevention, payments optimisation, and risk management. Hear our members share the value of MRC collaboration.

www.merchantriskcouncil.org



RISK
AND
PAYMENTS
INDUSTRY
DEVELOPMENT



RAPID Edu

**Essential Online Courses for
Fraud Prevention & Payments
Industry Professionals**

ENROLL TODAY!

merchantriskcouncil.learnupon.com



CHARGEBACK ESSENTIALS

Learn all about chargebacks, how to prevent them and protect your revenue.



FRAUD ESSENTIALS

Fight fraud with knowledge. Learn about fraud risks, how to detect and prevent fraud.



PAYMENT ESSENTIALS

Learn about payments, how to optimize them and increase payment acceptance.



About Kurt Schmid: Since 2020, Kurt Schmid is Marketing & Innovation Director Secure Digital Payments at Netcetera. Previously he has been responsible for the Digital Payment Division of Netcetera since the beginning of 2017. This resulted from the takeover of Nexperis GmbH, an Austrian mobile payment and NFC specialist founded by Kurt Schmid, who was CEO.

Kurt Schmid ■ *Marketing & Innovation Director Secure Digital Payments* ■ Netcetera

Improve conversion and reduce risk with current technologies

The COVID-19 pandemic is causing more and more people to buy more and more online. Despite previous reservations about ecommerce, many consumers have started shopping online for the first time. Before COVID-19, global ecommerce sales were expected to increase by 15% in 2020 compared to 2019. Now, it appears that this year's sales growth will be 25%. Therefore, it's of utmost importance to improve the conversion by making the checkout process as smooth as possible and at the same time use state of the art technology to reduce the risk.

However, the strong growth in ecommerce sales also carries with it an increased risk of fraud. In its **latest report on card fraud**, the European Central Bank reported that almost 80% of the total damage caused by card misuse was attributable to the card-not-present (CNP) sector, i.e. mainly to card transactions in ecommerce. Compared to 2017, card fraud in ecommerce has increased by almost 18%. This is one of the reasons why the EU Commission and the European Banking Authority (EBA) are making Strong Customer Authentication (SCA) mandatory under the current Payment Services Directive PSD2. This is intended to strengthen the confidence of consumers and merchants in ecommerce. However, this also means that consumers are increasingly being asked to authenticate themselves with a second factor, such as a one-time passcode (OTP) or a biometric feature.

Solving the contradiction between security and convenience

Until now, the contradiction between the highest possible level of security on the one hand and the smoothest possible user experience on the other seemed difficult to resolve. Now, the right technologies are available to meet the requirements of Strong Customer Authentication while providing customers with a simple and convenient checkout experience. This is particularly important for those consumers who are shopping online for the first time.

There are three simple and important processes:

1. The 3-D Secure process for card payments should be made as simple and streamlined as possible by optimising user procedures and also taking advantage of all available exemptions.
2. Tokenization offers an additional opportunity to increase the security of card payments in ecommerce.
3. With delegated authentication, online merchants can handle the authentication themselves and thus offer their customers a one-click checkout.

The use of exemptions using the 3DS 2.x protocol

In the context of PSD2, several possibilities exist to avoid Strong Customer Authentication to a large extent; for example, low value transactions with small amounts are excluded from SCA. The same applies for payments to merchants that are whitelisted by their customers. In addition, if a transaction risk analysis (TRA) is used, low risk card payments may be made without SCA. Finally, a 3-D Secure SDK is available to obtain additional data for risk management. →

With 3-D Secure, it is also important that all parties involved – merchants, PSPs and issuers – are aware of their respective responsibilities. To support online merchants in the transition to the latest version of 3-D Secure, Netcetera and Mastercard have set up a Merchant Testing Platform. This enables end-to-end tests to be carried out without much effort.

Network tokenization for a secure checkout

Many large online merchants already have extensive information about their customers. With card-on-file tokenization, they can permanently store card data in the form of tokens (a reference number that replaces the original card number PAN). Until now, PSPs used their own proprietary tokenization. However, it makes sense to use the network tokenization services offered by American Express, Mastercard, and Visa, as they offer a whole range of advantages. First of all, an end-to-end connection between card issuer and merchant can be established, which has a positive effect on the approval rate. Moreover, the checkout can display the customer's original card – not only the card number but also the card image to increase customer confidence. Security will be significantly enhanced by an additional cryptogram (as known from card present transactions). Experience to date shows that online merchants can improve their conversion rates by approximately 6% with network tokenization compared to normal card on file.

Delegated authentication for a PSD2 compliant one-click checkout

Online merchants can also use existing customer information for Delegated Authentication. As PSD2-compliant authentication methods for merchants, the FIDO-Alliance (Fast Identity Online) solutions are ideal. The FIDO standards for biometric authentication are supported

by Mastercard and Visa as well as by the most important OEMs and software providers (e.g. Microsoft, Samsung, Facebook, Apple, Google).

If a merchant has already securely registered its customers using a FIDO-compliant procedure, the login to the merchant's customer account can be used as authentication for payment transactions. Authentication via the card issuer is then no longer necessary. Merchants and card issuers can agree on this type of authentication through bilateral contracts. However, it seems more sensible and straightforward to use the services of Mastercard and Visa as Delegated Authentication brokers.

For the checkout, this means that customers are no longer pushed back and forth between the merchant app and the bank app, but can complete a payment with a single click, either via online or mobile channel only.

The bottom line is: there is a whole range of practical solutions available to online merchants that enable them to offer their customers both security and convenience. There is no doubt that all major online retailers will make consistent use of these new solutions. All other online merchants should follow as soon as possible in order to remain competitive.

The conclusion can be summed up as follows: if the right technologies are used and processes are optimised, the requirements of PSD2 and Strong Customer Authentication can be met without jeopardising conversion and without having to fear revenue loss.

About Netcetera: As market leader for 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.

www.netcetera.com

[Click here for the company profile](#)

Nok Nok

Walter Beisheim, Chief Business Development Officer for Nok Nok Labs, discusses the importance to deliver consistent and secure SCA in both mobile apps and browsers.



About Walter Beisheim: Mr Beisheim has over 30 years of experience as a senior executive in leading public and private companies in the Information Technology industry that provide products and services in the AI, NLP, online security, mobile technology, and fraud prevention solutions sectors. In his role as Chief Business Development Officer for Nok Nok Labs, he is responsible for business development strategy and identifies, and executes on opportunities to expand Nok Nok's global relationships with customers and partners.

Walter Beisheim ■ Chief Business Development Officer ■ Nok Nok

On your website, you say that 'Nok Nok has solved the consumer authentication (a.k.a. SCA) problem'. Can you describe what that problem is, and give some examples of the companies for whom you have solved that problem?

Three basic categories create vulnerabilities, and increase cart abandonment with legacy authentication techniques:

- 1) Shared secrets like passwords, PINs, and KYC answers are stolen by fraudsters, and forgotten by purchasers.
- 2) Attempts to overlay passwords with step-up, primarily SMS OTP are also vulnerable to man-in-the-middle, and SIM Swap, as well as often resulting in cart abandonment.
- 3) The lack of security in the communication channel between the merchant and the purchaser's device to prevent fraudsters from 'intruding' is the third major exposure of legacy authentication.

“The future of new and innovative identity authentication applications is as close to us today as the realisation of self-driving vehicles, which is already available from companies like Tesla.

Nok Nok's FIDO-based solution solves these problems by replacing passwords with secure and simple authentication measures such

as fingerprint and device ID. Our solution is convenient for users and complies with regulations like PSD2 SCA. This solution to the consumer authentication problem is backed by Apple, Google, Microsoft, Mastercard, and Visa, as well as other major industry participants.

How is your solution different from the 'legacy risk scoring solutions'? Also, what has Nok Nok done to ensure that your solution works together with 3DS and other standards (e.g. W3C)?

Risk scoring solutions employ different forms of inference algorithms that attempt to identify the probability that an online transaction is fraudulent. For example, the system may 'infer' that the purchaser is who they claim to be based on their IP address, and because they hold their device, or type on their device consistent with the last transaction from that purchaser. This is a simplification, and many modern risk scoring systems are very sophisticated, but they all are still basically inference engines that generate probability.

Nok Nok's authentication solution generates a 'yes/no' indication that the purchaser has passed a strong, multi-factor authentication challenge. This indicator is returned based on a single, frictionless 'gesture' from the user such as touching their fingerprint sensor. If the indication returns 'no', the customer is asked to authenticate on one of their trusted devices. This binary approach takes much of the 'guesswork' out of identifying fraud. Additionally, FIDO authentication does not store any of the user's PII on a server. →

Nok Nok not only supports W3C web authentication and EMVCo 3DS standards, but we have also been a key contributor to the creation of these standards. As a result, FIDO integration with 3DS to provide Secure Customer Authentication, and to facilitate Delegated Authentication by merchants is supported by EMVCo, and the W3C standard adds support for web browsers as well as mobile apps for this purpose.

Can you give some examples of how your customers are applying your solution to more than one use case, and more than one channel?

Many of our long-term, early adopter customers were Mobile Network Operators (MNOs). They all started using Nok Nok for login auth to reduce password resets and to reduce account takeovers. From there, they have added various additional use cases such as purchase approval as a service for merchants, and access to the MNO's customer service without requiring the subscriber to answer a dozen questions before receiving assistance. More recently, Nok Nok authentication is being used by tier one US operators in their ZenKey third-party cross-carrier identity service.

With the introduction of the W3C standard supporting FIDO authentication in all major browsers, all of our customers have plans to add web browser authentication for phones, tablets, and PC devices to their existing mobile app delivered solutions. We have added this support without any requirement to modify the mobile app-based solution they are already using. Today, with the way that Apple, Google, and Microsoft have implemented FIDO, a user only needs to be registered once to use multiple channels on the same device.

How can banks, merchants, and PSPs evaluate and compare 3DS authentication options?

Nok Nok has direct relationships with banks globally to deliver their comprehensive authentication solution, including payments authentication. For merchants in Europe, Mastercard has identified Netcetera as their 3DS testing partner for PSD2 compliance. Netcetera and Nok Nok have partnered to deliver a '3DSCA' solution through the integration of Nok Nok's solution with Netcetera's 3DS services.

What is the future for password-less SCA and how can a PSD2 SCA solution that is implemented today benefit a merchant in other areas tomorrow?

While the ability to deliver consistent and secure SCA in both mobile apps and browsers is a game changing capability for online merchants, the benefits do not end there. Nok Nok's auth solution can enable a merchant to provide more customer convenience and trust in every service they deliver online. A FIDO registration can also be used as a secure and convenient method for POS transactions, ATM transactions, kiosk delivered services, and IoT based services. Nok Nok already delivers support for wearables possession auth on both Apple Watch and Wear OS. We also have the capability to 're-use' the authentication registration created for an online service within an IoT device; for example an entry control turn-style, or even a car share service. The future of new and innovative identity authentication applications is as close to us today as the realisation of self-driving vehicles.

As with the other authentication innovations, Nok Nok will continue to be at the forefront in delivering the benefits of real industry solutions.

About Nok Nok: Nok Nok provides secure, scalable, and frictionless experiences for passwordless authentication, preventing fraud and security risks. By reducing the reliance on weak, phishable passwords, Nok Nok empowers organisations to improve the authentication experience, while meeting the most advanced security and regulatory requirements. Customers include cloud, mobile, and IoT businesses. For more information, visit www.noknok.com.

www.noknok.com

[Click here for the company profile](#)



About Ed Whitehead: Ed Whitehead is the Managing Director, Europe, for Signifyd, where he leads a team dedicated to the expansion and support of Signifyd's European client base. Prior to joining Signifyd, Ed worked at Gigya, SAP and Experian accumulating extensive knowledge across data and legislation in identity, fraud, ecommerce, and customer experience.

Ed Whitehead ■ *Managing Director, Europe* ■ Signifyd

Although Europe's revised Payments Services Directive (PSD2) went into effect in September 2019, the deadline for enforcement of Strong Customer Authentication (SCA) has since been extended, once across Europe as a whole and twice in the UK. These delays are the result of persistent lobbying from merchants and the payments community who feel that SCA will cause them to lose customers in a time when many are hurting from the economic consequences of COVID-19.

This sentiment is not surprising or unwarranted. By **Visa's estimations**, SCA could lead to a 30% increase in cart abandonment due to the friction it places at checkout. And Signifyd's testing shows the legacy SCA protocol – 3DS 1 – can add 15 seconds or more to the checkout process, which in ecommerce feels like a lifetime.

Sentiments aside, as of January 2021, European merchants will have to face the music once and for all when SCA compliance becomes mandatory. For those who have already implemented 3DS 1, it may be tempting to ignore the looming deadline given the legacy protocol's compliance with PSD2. However, there is a business case to be made for upgrading to 3DS 2 – get it right and you could be looking at as much as a 6% lift in revenue AND a built-in leg up on competitors who don't.

3DS 1 vs 3DS 2 – what's the difference?

The 3DS 1 protocol was established back in 2001. At that time, many merchants were unable to process card-not-present (CNP) payments due to the increase in fraud pressure it presented and payment processors' reluctance to work with risky businesses.

Following 3DS 1, every transaction must be authenticated regardless of risk level. In practice, this means redirecting consumers to a new window in order for them to manually provide additional identity-verifying information – usually in the form of a one-time passcode.

In tandem with the roll-out of PSD2, EMVCo was commissioned to develop the new and improved 3DS 2 protocol. 3DS 2 comes with several key updates, the biggest being that it differentiates between high and low risk transactions and allows for some SCA exemptions based on perceived risk.

3DS 2 is a language that can be spoken well – or not

A recent Visa study tied 3DS 2 implementation to a **70% decrease in cart abandonment and 85% reduction in transaction time**. However, it's not simply implementing the protocol that yields these results; rather, the most successful deployments optimise exemptions and minimise authentication step-ups.

There are two components of a strong payments compliance strategy in particular that merchants will need to get right: Transaction Risk Analysis (TRA) and Intelligent Routing. TRA is a process for assessing the risk of a purchase prior to authorisation by the payment processor. Ability to perform this – and perform it well – requires insight into a consumer's shopping behaviour and past transactional data, which can be nearly impossible if a consumer is new to a merchant. →

Signifyd's approach to TRA is predicated on our Commerce Network, which includes transactional data from tens of thousands of merchants around the globe. This comprehensive dataset means that 98% of orders sent to Signifyd for review are placed by consumers we've previously seen within our merchant network and, combined with our machine learning algorithms, allows us to instantly identify fraudulent orders pre-authorisation.

If TRA identifies a low risk transaction, and the merchant has demonstrated a low rate of fraud over time, an exemption can (and should) be requested. Here, again, Signifyd technology comes into play to help us intelligently route orders down the path of least resistance – in this case, one in which no authorisation step-ups are required at all.

But what if exemption qualifications are not met? Are all SCA-bound transactions doomed to poor customer experience and high cart abandonment? Not if authorisation step-ups are performed dynamically, opting for the most seamless route at every stage.

Performing SCA seamlessly gives you a built-in competitive advantage

The way you execute SCA has the power to make or break your customer experience. According to PSD2 regulation, if a step-up is required, a customer must verify their identity in two of three ways: with something only they know (i.e. a password), with something they possess (i.e. a device), and with something inherent to them (i.e. a fingerprint or keystrokes). Partnering with a 3DS 2.2 vendor who can perform these additional layers of authentication discreetly, without the consumer lifting a finger, is an essential component of seamless SCA.

Signifyd's aptly named Payments Compliance solution Seamless SCA allows merchants to passively conduct SCA while customers shop on their site, by measuring device token information to satisfy the possession element and behavioural and biometric information to satisfy the inherence element. Our built-in 3DS 2.2 capabilities ensure that a merchant's payment provider and the cardholder's issuing banks receive the information necessary to authenticate the transaction.

Hence, the great results: after replacing their legacy 3DS 1 implementation, Signifyd customer Emma Mattress recovered an additional 6.4% in revenue thanks to a higher order approval rate and lower incidences of cart abandonment.

The case for 3DS 2 implemented well boils down to a competitive advantage for consumers' business and the brand loyalty that brings them back for more. Conversely, what's at risk with remaining on 3DS 1 is even more revenue leakage as customers flock toward competitor sites that offer a more enjoyable shopping experience.

About 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.

www.signifyd.com

[Click here for the company profile](#)

MK2 Consulting

The Future of Fraud After PSD2's Strong Customer Authentication Deadline



About Jonathan Williams: Jonathan is an independent advisor in interbank and card payments. He has led product management in successful start-ups in cybersecurity, telecommunications, and enterprise software industries and his current focus is on identity, financial crime, Open Banking, and compliance.

Jonathan Williams ■ Independent Advisor ■ MK2 Consulting

No one in the European payments industry will be unaware that Strong Customer Authentication (SCA) is coming or is already here, although the deadlines vary between the UK and EU/EEA. It's a tale of two industries: personal and business banking is compliant already but there is room for improvement, while the cards industry is still aligning the different parties – merchants, acquirers, issuers, card-holders – so that it all works seamlessly for ecommerce.

As a physicist, I am used to natural laws. One which I'd not come across in science is the Conservation of Fraud. Like the Conservation of Energy, it says that the effort expended using fraud to extract value is (fairly) constant, while losses go up and down depending on the effectiveness of prevention measures. Fraudsters don't simply give up when we make it harder for them, they just look for the next easiest route.

What will happen to fraud?

So when we ask what will happen, we need to consider not only the first-order effects – what will PSD2 do to the fraud it targets – but also the second- and third-order effects of what criminals will try next.

Firstly, will SCA be successful? There is no reason to assume that, correctly implemented, it will not. The risk is that, by looking for loopholes in the law to make payments frictionless for consumers, we may make it easier for criminals. This is the logic which chooses known-insecure, SMS-based one-time passwords over secure tokens. In addition, there are exceptions, for example payments initiated through acquirers outside the PSD2-zone for which SCA is not mandatory (although it will be good practice).

Secondly, criminals will look to frauds which SCA does not address. Many countries, including the UK, have seen the growth of 'push payment' attacks which (re-)direct payments to an account in criminal control. **Estimates in the UK alone are of billions of pounds lost per year** and, because the payment is made by the genuine business or personal customer, SCA cannot prevent it. Measures such as confirming the name and address of an account before initiation can help, but the move to instant SEPA payments in Europe puts all providers under time pressure.

PSD2 also allows third parties to access payment accounts using 'Open Banking' or XS2A interfaces. Broadly, this allows customers to benefit from services using banking data and payments that banks could not afford to develop individually. Personal financial management, retail payments, and improved credit scoring are merely three possible applications. There are, however, weaknesses in the trust scheme which could mean that fraudsters can obtain SCA credentials to take over a customer's account.

As an example, criminals could develop a website purporting to be a real or fictitious 'third-party provider'. As part of signing up, they could request the customer's SCA login information but instead of using it for 'Open Banking', they could transmit it to the bank in their own online banking session, pretending to be the customer. This might allow them to login, re-issue cards, make transfers, or set up scheduled payments. Alternatively, they could change security information including address, e-mail, and challenge questions to lock out the genuine customer while they emptied the account. →

The measures to minimise this are simple:

- standardisation of processes;
- consistent user experiences;
- education of customers;
- better analysis of operational data;
- improved authentication mechanisms.

Criminals benefit when there is confusion. If a customer does not know what to expect, they will accept whatever they are told, whether by a payment service provider or a criminal. Time and again, the payments industry has failed its customers by not informing them well or early enough.

Data is also a key weapon to fight fraud. 3-D Secure 2.0, the new communication standard adopted by the card schemes to support authentication, allows more data to be provided by merchants to issuers. This includes fields like the customer's e-mail address so the issuer can check if it's one of the customer's known addresses. But issuers are in danger of drowning in data and thereby failing to spot tell-tale signs. Automated analysis and especially machine learning or AI can help make sense of this new data, but new technology will require supervision and explanation to the regulator. Ensuring algorithms that are unbiased will be a key challenge as we start to use them.

Finally, criminals will be attempting to get around SCA technologies so payment services providers must be on their guard to identify weaknesses early, patch, or retire compromised mechanisms and look to new technologies such as behavioural biometrics to secure transactions.

So, will fraud losses go down or up? While the fraudsters will continue to expend effort, losses to payment fraud could decrease, but only if we are all focussing on the right outcomes. Technology on its own will not solve the problem but it can help us move in the right direction.

About MK2 Consulting: We provide financial organisations with the clarity they need to understand the impact financial crime prevention, identity management, and payment operations have on their business. Our in-depth knowledge and independent advice help you analyse your operations and adopt the right strategies to improve efficiency, increase revenue, and ensure regulatory compliance.

www.mk2consulting.co.uk

Wargaming

About Fraud and Strong Customer Authentication – Old Challenges, New Patterns



About Elena Emelyanova: Elena Emelyanova is a Senior Payments and Fraud manager at Wargaming. While heading Acquiring team within Wargaming, she specialises in ecommerce acquiring and fraud protection globally, having a strong understanding of various markets throughout Europe, North/South America, Asia, and CIS. With the benefit of working at a mobile carrier company for 4 years before joining Wargaming team and a 4 years background of leading NA/LATAM payments team at Wargaming, Elena helps Wargaming to optimise the card payments and alternatives flows all over the world, as well as keeping the fraud level low. Her total experience in payments industry is of 8 years.

Elena Emelyanova ■ Senior Payments and Fraud Manager ■ Wargaming

Wargaming is an online game developer and publisher. Our games are free-to-play, and our business model is based on micro transactions. Moreover, the way our games are created doesn't offer the possibility to do in-game fraud, because one may not resell the purchased item (once you bought it, it's yours), and we do not do cash out.

The gaming industry, among others, is indeed facing a big challenge again this year, especially because the mandated implementation of Strong Customer Authentication (SCA) has been postponed from the last year and now we are impatiently looking forward to what will happen after the 31st of December 2020.

Why is SCA compliance still a challenge

3DS 2.0, the next generation of the current customer authentication protocol, should bring security and trust to ecommerce transactions, and naturally, remove or at least decrease fraud. That's a great initiative especially taking into consideration the increasing global trend of ecommerce fraud. However, it seems it's not that easy to implement it. In order to reach the goal, every stakeholder (merchant, PSP, or acquirer and issuer) needs to do their part respectively in order for the whole ecosystem to benefit from SCA.

Wargaming has been ready to support 3DS2 since last year, however, this doesn't guarantee we will be protected from fraud after 31st of December. The inconsistency in readiness with SCA still remains, plus the lack of comprehensible statistics, predictions

in conversion decrease, and a lot of open questions which still cannot be answered – that's from one side. From the other side, the upcoming peak season with the highest sales (Black Friday, Christmas) = the highest potential fraud time.



Therefore, here are the main challenges Wargaming has been facing so far prior to the SCA deadline, which are also very common for each merchant looking to stay relevant and compliant on the market:

1. There is a lot of inconsistency in industry readiness. As a merchant, we are mostly interested in issuer readiness, after making sure, of course, that our acquirers are compliant. Unfortunately, despite of multiple EBA letters and each EU country national bank authorities' notices – the overall readiness (I mean not just on paper) is far from being 100% complete. On the other hand, hearing questions from merchants like 'which transactions are considered to be in scope?' or 'will SCA be mandatory only in EU as per new regulation?' – just show that there is also a significant gap in merchants' awareness and readiness. →

2. Despite of the fact that we do have already transactions going via 3DS2 request – there is no clear and easy-to-reach analytics we can use in order to estimate the level of customers' involvement, results, of issuers reaction etc. Neither our technical side, nor our acquirers are ready at the moment with supporting analytical side of the project.
3. Companies caring a lot about friction in the payment flow/customer payment journey are all preparing for conversion decrease. With the introduction of an extra step in the authentication process, that's the logical estimation. Luckily, there will be exemptions, but, there is a huge BUT again. Exemptions are available only in 3DS2.2 version (which is mandatory to be implemented by the end of 2020), and can function only in case issuers are ready to support them.
4. A lot of open questions with no answers. Well, I believe we'll need to learn from our own experience in 2021.



New fraud patterns at the horizon


In addition, a few words to add about the current situation with fraud. We do see new patterns emerging this year, absolutely new approaches, which literally means that fraudsters are always one step ahead. Or, at least, they try to. Thanks to the tools we are using and thanks to our payment partners we manage to identify them and prevent their future fraudulent activities. In 2021, the situation will not change much I believe, at least not in the first half-year period. SCA will not be fulfilling its function in full up until the whole industry is compliant and fine tunes all the processes related to it.

About Wargaming: Wargaming is an award-winning online game developer and publisher headquartered in Nicosia, Cyprus. Operating since 1998, Wargaming has grown to become one of the leaders in the gaming industry with 4500+ employees and offices spread all over the world. Over 200 million players enjoy Wargaming's titles across all major gaming platforms.

www.wargaming.net



Company Profiles

Company	4Stop (Fourstop GmbH)
	<p>4Stop provides global KYB, KYC, compliance, anti-fraud, data science, and monitoring technology – available from one API. Businesses access thousands of data services with real-time activation backed behind customised and dynamic cascading verification and decision-making frameworks. Establishing a centralised view-of-risk saving businesses money and resources managing risk data and operations.</p>
<p>Website</p> <p>Technology</p> <p>Target market</p> <p>Contact</p> <p>Geographical presence</p> <p>Year founded</p> <p>Service provider type - category</p> <p>Member of industry association and/or initiatives</p> <p>Company's motto</p>	<p>4stop.com</p> <p>Cloud enabled API On-premises</p> <p>Financial institutions Payment services providers Acquirers Merchants/ecommerce Fintech Government services Online communities/web merchants Crypto businesses FX platform business Other online businesses</p> <p>Sales@4stop.com info@4stop.com</p> <p>Global</p> <p>2016</p> <p>Data provider and verification Digital identity service provider Customer verification Business verification/underwriting Technology vendor Web fraud detection company Verification-as-a-Service (VaaS) Merchant risk/Transaction laundering prevention</p> <p>Yes</p> <p>To provide a simple, modern, fail-safe, and all-in-one risk management tool that brings future-proofed sustainability on mitigating global risk for online entities.</p>
Services	
<p>Unique selling points</p> <p>Pricing model</p> <p>Fraud prevention partners</p> <p>Other services</p> <p>Third party connection</p>	<p>4Stop leverages its platform to enable merchants to screen for multiple fraud use cases, including onboarding and payment. Our orchestration hub allows for efficient, cost-effective and frictionless verifications of customers and businesses. Paired with dynamic decision-making frameworks and fully customised compliance workflows merchants have an end-to-end solution to confidently mitigate risk, always.</p> <p>Pricing is per 'Core Service' and/or 'Verification KYC' transaction and based on volume and complexity.</p> <p>ComplyAdvantage, Jumio, TransUnion</p> <p>Verification/Authentication/Validation – KYB/KYC data services</p> <p>N/A</p>
Technology: Identity verification methods	
	<p>Geo-location check, phone ID check, device ID, BIN check, breached email check, email verification, physical address check, compliance watchlist screening and real-time continuous monitoring, adverse media, identity document scanning and live video, biometric identity verification, personally identifiable information (PII) validation, credit check, business ID verification, business compliance, business web analysis, transaction verification, card verification value, account association logic, and whitelist/blacklist database</p>
<div>View company profile in online database</div>	

Authentication technology used	
	Geo-location, remote access detection, device intelligence, knowledge-based authentication, phone 4-pin, facial biometrics, payer and receiver authentication, behavioural analysis, behaviour biometrics, data analytics, cascading verification logic, dynamic anti-fraud frameworks, mobile app push, hardware token, and one-time passwords
Authentication Context	
	Online Mobile
Reference Data connectivity	
Connectivity to governmental data	Citizens register, company register, IDs
Other databases	Commercial attribute providers, credit databases, utility, phone service providers, sanctions lists, banks
Clients	
Main clients/references	Mifinity, Draglet, Gatehub, Paysend, Paymentz, eMerchantPay, Paytah by Monetum, BCCS, Hexopay
Future developments	Machine learning/enhanced smart rules hub Enhanced KYB/KYC solutions On-going data aggregation and integrated KYB/KYC data services Enhanced UI/UX experience



Know Your Risk. Always.

Access the largest KYB, KYC and fraud prevention data hub worldwide with dynamic intelligence and enrich your risk mitigation instantly.



**HUNDREDS
OF KYB/KYC
DATA SOURCES**



**DATA-DRIVEN
BUSINESS
UNDERWRITING**



**FUTURE-PROOF
COMPLIANCE
WORLD-WIDE**



**INTELLIGENT
ANTI-FRAUD
MANAGEMENT**




**TRANSACTION
MONITORING &
INTELLIGENCE**

Obtain premium and automated fraud defence tailored to your exact risk needs globally to reduce operation and data resources, all while having future-proofed sustainability.

4STOP

The Last API You Need To Manage Risk.

Company	Accertify, Inc., an American Express Company
	<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>
<p>Website</p> <p>Technology</p> <p>Target market</p> <p>Contact</p> <p>Geographical presence</p> <p>Year founded</p> <p>Service provider type - category</p> <p>Member of industry association and/or initiatives</p> <p>Company's motto</p>	<p>accertify.com</p> <p>On-premises Cloud enabled Hybrid</p> <p>Merchants/ecommerce (retail) Airlines Travel and hospitality Banks/FS Ticketing and Entertainment Online communities Online gaming PSP Ride sharing Corporate Fintech Other online businesses</p> <p>Michelle DiDomenico: mdidomenico@accertify.com</p> <p>North America, LATAM, APAC, EMEA</p> <p>2008</p> <p>Fraud platform Consumer authentication ID verification Data provider and verification Chargeback management Merchant risk/Transaction laundering prevention Digital identity service provider Technology vendor Web fraud detection company Payment service provider (PSP) Issuer Acquirer</p> <p>MRC, FIDO, AICPA (SOC), IATA, MAG, Airline Information Organization, and more</p> <p>We help to solve your digital identity and financial fraud risks, making it simpler to protect your organisation.</p>
Services	
<p>Unique selling points</p> <p>Pricing model</p> <p>Fraud prevention partners</p> <p>Other services</p> <p>Third party connection</p>	<p>Platform that addresses the entire customer journey from account creation, authentication, account activity, purchase, payment, and dispute management: Risk engine – execute rules and machine learning algorithms; Device intelligence – mobile app and browser; Reputational community database; Professional services – industry expert consultation; Integrated third-party vendors.</p> <p>Transaction based pricing</p> <p>American Express, Mastercard, Emailage, Ekata, Amadeus, FreedomPay, and more</p> <p>Secure communication, PSD2/SCA, account takeover, new account opening, payment fraud prevention, frictionless authentication, bot detection, user behaviour analytics</p> <p>For more information please contact Accertify.</p>
<div>View company profile in online database</div>	

Technology: Identity verification methods	
	Personally Identifiable Information (PII) validation, email verification, phone verification, social verification, credit check, compliance check, reputation/history verification, behavioural biometric, device intelligence
Authentication technology used	
	Password/phrase, one-time password, digital certificates
Authentication Context	
	Online Mobile ATM Call centre
Reference Data connectivity	
Connectivity to governmental data	Yes
Other databases	No
Clients	
Main clients/references Future developments	<p>Please see our website (www.accertify.com) for list of clients.</p> <p>A strong focus on a new Delegated Authentication solution, using the 3DS 2.2 specification and FIDO2 capabilities to allow merchants to maximise liability shift while minimising customer friction traditionally associated with 3DS. Our solution will combine best-in-class device ID, biometric sensor data and our Payment Gateway capabilities to provide merchants with an effective approach to Strong Customer Authentication.</p>




Up Your Game Against Fraud

Accertify is a leading provider of fraud prevention, chargeback management, SCA optimisation, digital identity and payment gateway solutions to customers spanning financial services, retail, airlines, travel, ticketing and entertainment industries worldwide. Accertify's layered risk platform, machine learning backbone, and rich reputational community database enable businesses the ability to address challenges across the entire customer journey without impacting the customer experience.

www.accertify.com

Accertify
AN AMERICAN EXPRESS COMPANY



Company	ACI Worldwide
	<p>ACI Worldwide delivers mission-critical real-time payment solutions that power omni-commerce and ecommerce payments while managing fraud and risk. We are driving the digital transformation of merchants and PSPs to help them meet the real-time payment needs of their consumers and business customers.</p>
<p>Website</p> <p>Technology</p> <p>Target market</p> <p>Contact</p> <p>Geographical presence</p> <p>Year founded</p> <p>Service provider type - category</p> <p>Member of industry association and/or initiatives</p> <p>Company's motto</p>	<p>www.aciworldwide.com</p> <p>Native cloud SaaS</p> <p>Merchants/ecommerce (telecom, gaming & digital goods, retail, travel) Corporate Fintech Acquiring banks PSP/MSP SMBs Telecom</p> <p>amanda.mickleburgh@aciworldwide.com</p> <p>Global</p> <p>1975</p> <p>Fraud platform Consumer authentication Chargeback management Merchant risk/Transaction laundering prevention</p> <p>MRC, IMRG, Vendorcom, MAG</p> <p>Any Payment, Every Possibility</p>
Services	
<p>Unique selling points</p> <p>Pricing model</p> <p>Fraud prevention partners</p> <p>Other services</p> <p>Third party connection</p>	<p>Multi-layered ecommerce and mcommerce fraud solution focused on enabling merchants to sell more and lose less: industry leading KPIs; patented incremental machine learning models; rich, global consortium data; support from expert risk analysts as an inclusive part of the service.</p> <p>Pricing is per transaction and based on volume and complexity or SaaS-based pricing model.</p> <p>Including Arvato, Ekata, iovation, Neustar, Perseuss, emailage, Threatmetrix</p> <p>Independent ecommerce payments gateway connecting to 250+ acquirers and APMs, including pay later methods</p> <p>To partners as above</p>
Technology: fraud prevention methods	
	<p>ACI offers a multi-layered fraud prevention solution. This combines advanced machine learning models with positive profiling capabilities, global fraud intelligence, and multi-channel strategies to increase conversion while reducing fraud and chargebacks. The solution includes integrated third-party services including manual reviews and chargeback management. Designated expert risk analysts with global experience are an inclusive part of the service and work closely with customers to tailor fraud strategies by product, channel, market sector, and geography.</p>
<div data-bbox="1066 2040 1524 2085">View company profile in online database</div>	

Company	Arkose Labs
	<p>Arkose Labs bankrupts the business model of fraud. Recognised by Gartner as a 2020 Cool Vendor, its innovative approach determines true user intent and remediates attacks in real time. Risk assessments combined with interactive authentication challenges undermine the ROI behind attacks, providing long-term protection while improving good customer throughput.</p>
<p>Website</p> <p>Technology</p> <p>Target market</p> <p>Contact</p> <p>Geographical presence</p> <p>Year founded</p> <p>Service provider type - category</p> <p>Member of industry association and/or initiatives</p> <p>Company's motto</p>	<p>www.arkoselabs.com</p> <p>Native cloud</p> <p>Banks / FS</p> <p>Corporate</p> <p>Fintech</p> <p>Merchants / ecommerce</p> <p>PSP/acquirers</p> <p>SMBs</p> <p>Telecom</p> <p>Lizzie Clitheroe: l.clitheroe@arkoselabs.com</p> <p>Global</p> <p>2016</p> <p>Fraud platform</p> <p>Consumer authentication</p> <p>MRC</p> <p>Bankrupting the Business Model of Fraud</p>
Services	
<p>Unique selling points</p> <p>Pricing model</p> <p>Fraud prevention partners</p> <p>Other services</p> <p>Third party connection</p>	<p>Arkose Labs determines true user intent by analysing traffic for behavioural telltales of fraud and testing suspicious traffic using interactive challenges. This eliminates automated attacks and wastes fraudsters' time, making attacks financially non-viable. Good users rarely see challenges, but if they do, throughput rates beat any other step-up authentication.</p> <p>SaaS-based pricing</p> <p>Information available upon request</p> <p>Managed service</p> <p>Open platform with simple integrations with third party tools</p>
Technology: Identity verification methods	
	Proprietary telltale database
Authentication technology used	
	IP reputation, device ID, network forensics, embedded machine learning, geo-location, rate limits and velocity, behavioural biometrics, user interaction data, 3D visual enforcement challenges
Authentication Context	
	Online Mobile Other - gaming consoles
Reference Data connectivity	
Connectivity to governmental data	N/A
Other databases	IP reputation, geo-location
Clients	
Main clients/references	Microsoft, GitHub, EA, Roblox
Future developments	Information available upon request
View company profile in online database	



Arkose Labs




DOWNLOAD THE Q4 2020 FRAUD AND ABUSE REPORT

Data-driven analysis of 2020 fraud trends and the impact of COVID-19

www.arkoselabs.com/fraudreport



Company	Covery
	Covery is a simple all-in-one KYC, AML, and fraud prevention tool for risk analysts, payment managers, AML specialists, BI professionals, and data scientists developed to mitigate the risks of fraud encounter and increase business revenue.
Website	https://covery.ai/
Technology	Cloud enabled
Target market	Fintech Corporate Merchants/ecommerce PSP/acquirers SMBs Gambling, betting, iGaming, e-learning, dating
Contact	sales@covery.ai , marketing@covery.ai
Geographical presence	Global
Year founded	2016
Service provider type - category	Fraud platform Chargeback management Merchant risk/Transaction laundering prevention
Member of industry association and/or initiatives	No
Company's motto	Fraud shall not pass!
Services	
Unique selling points	What we offer: - client data acceptance; - rule-based and machine learning hybrid; - deep customisation; - actual solutions; - free trial; - functionality to work with loyal users to increase revenue.
Pricing model	Various pricing plans for small and large businesses are available. Most of pricing plans are based on the volume of Decision API calls.
Fraud prevention partners	Ondato, ShuftiPro, Verifi, Dow Jones
Other services	N/A
Third party connection	Dow Jones, Verifi, Ethoca
Technology: Identity verification methods	
	Identity document scanning, video scanning, Personally Identifiable Information (PII) validation
Authentication technology used	
	Device fingerprinting, BIN lookup, geo-location, watchlists, KYC, behavioural analysis, machine learning, data analytics
Authentication Context	
	N/A
Reference Data connectivity	
Connectivity to governmental data	No
Other databases	Dow Jones watchlists
Clients	
Main clients/references	Genome, UniPay, Fastshift (Betconstruct), Mobeetech, Mr.Bet, Boosta, AskFm
Future developments	More information upon request

[View company profile in online database](#)



Power your risk team

And maximize revenue with more adaptive fraud analysis

The mission of Covery is to provide a simple all-in-one tool to solve complex tasks of various teams.

Here are some benefits you'll get with Covery:

Global database Trustchain

With Trustchain business cuts down the number of bots and fraudsters up to 40% having just reputation records of 12 user identifiers: Email, Card ID, Phone, IP, Email domain, System account ID, etc.

Device Fingerprinting


Device Intelligence technology designed by Covery that collects device data during any step of user journey and secures business from synthetic identities, account takeovers, identity thefts, and CNP fraud.

Customizable rules and ML models


Under the hood, Covery uses Supervised Machine Learning that gives unlimited capabilities for creating custom ML models with no development resources to create a specific risk logic.

KYC/KYB/AML Automation

Covery confirms AML safety and helps to comply with all the regulatory standards with a one-time screening and ongoing monitoring of users through the International watchlists.

Company	Cybersource
 <p>cybersource A Visa Solution</p>	<p>Cybersource helped kick start the ecommerce revolution in 1994 and haven't looked back since. Through global reach, modern capabilities, and commerce insights, we create flexible, creative commerce solutions for everyday life – experiences that delight customers and spur growth globally. All through the ease and simplicity of one digital platform to manage all payment types, fraud strategies, and more. Knowing we are part of Visa and their security-obsessed standards, you can trust that business is well taken care of – wherever it may go.</p>
<p>Website</p> <p>Technology</p> <p>Target market</p> <p>Contact</p> <p>Geographical presence</p> <p>Year founded</p> <p>Service provider type - category</p> <p>Member of industry association and/or initiatives</p> <p>Company's motto</p>	<p>www.cybersource.com</p> <p>Cloud enabled Native cloud</p> <p>Banks/FS Corporate Fintech Merchants/ecommerce PSP/acquirers SMBs Telecom</p> <p>www.cybersource.com/contact_us</p> <p>Global</p> <p>1994</p> <p>Fraud platform Consumer authentication ID verification</p> <p>Merchant Risk Council, Vendorcom, Association of Certified Fraud Examiners. Cybersource has been granted 90+ patents.</p> <p>Flexible, creative commerce solutions for everyday life</p>
Services	
<p>Unique selling points</p> <p>Pricing model</p> <p>Fraud prevention partners</p> <p>Other services</p> <p>Third party connection</p>	<p>Drawing on intelligence from over 68 billion global Visa transactions, backed by real-time machine learning (ML) plus our own experts, we incorporate merchant data with these insights and apply to their business. More options, via a combined AI/ML and rules-based solution, help merchants design and test in real-time. And a more complete approach means our customers benefit from a truly integrated platform, that handles everything from gateway capabilities and tokenization to payer authentication, and much more.</p> <p>Tiered SaaS-based pricing model</p> <p>ThreatMetrix, Cardinal Commerce, Neustar, Ekata, and Emailage</p> <p>Managed services, analytics, identity validation, account takeover protection, export compliance, delivery address validation</p> <p>Cybersource has connections with a global ecosystem of financial institutions, solution providers, and technology partners, including SAP, Salesforce, Magento, Zuora, Amadeus, Sabre, and many more.</p>
Technology: Identity verification methods	
	<p>Address verification services, CNP transactions, Card Verification Value (CVV), BIN lookup, geo-location checks, device fingerprint, payer authentication, velocity rules – purchase limit rules, white list/black list database, 3-D Secure – authentication, machine learning, data analytics, name/address/phone validation services available</p>
Authentication technology used	
	<p>Cybersource's Payer Authentication uses the Cardinal Commerce API to authenticate transactions for 3-D Secure. Merchants can run authorisation in our Decision Manager tool prior to fraud screening, meaning results can be included in rule building capabilities. In doing so, we help maximise 3-D Secure benefits to merchants without compromising the customer experience.</p>
View company profile in online database	

Authentication Context	
	Online Mobile POS Call centre Other – more information upon request
Reference Data connectivity	
Connectivity to governmental data	Yes
Other databases	We connect with other commercial attribute providers for identity validation, such as LexisNexis' Accurant.
Clients	
Main clients/references	Rue du Commerce, ghd, Cinépolis, DICK'S Sporting Goods
Future developments	For more information you can reach us at: www.cybersource.com/contact_us .



Choosing between
chargebacks and
false positives?


Choose neither.

Build fraud strategies
that get more business in.



cybersource
A Visa Solution

www.cybersource.com

Company	Entersekt
	<p>Entersekt is a leading provider of device identity and customer authentication solutions. Its multi-patented, regulatory compliant technology helps financial institutions and other enterprises to build trust and boost loyalty with secure, convenient, and engaging new digital experiences.</p>
<p>Website</p> <p>Technology</p> <p>Target market</p> <p>Contact</p> <p>Geographical presence</p> <p>Year founded</p> <p>Service provider type - category</p> <p>Member of industry association and/or initiatives</p> <p>Company's motto</p>	<p>www.entersekt.com</p> <p>On-premises Cloud enabled Native cloud Hybrid</p> <p>Financial institutions Card issuers Insurers Payment service providers</p> <p>Entersekt sales team: sales@entersekt.com</p> <p>Africa, Europe, Middle East, North America</p> <p>2008</p> <p>Consumer authentication</p> <p>FIDO Alliance; W3C; EMVCo; Emerging Payments Association; WASPA; Mobey Forum; Mobile Connect; US Payments Forum</p> <p>The power of trust</p>
Services	
<p>Unique selling points</p> <p>Pricing model</p> <p>Fraud prevention partners</p> <p>Other services</p> <p>Third party connection</p>	<p>Patented digital certificate technology (closed PKI) deployed at scale – on the mobile and browser; out-of-band, secure communication via trusted channel; mutually secured, end-to-end encryption via our own crypto stack; transaction context and strong customer consent; secure customer engagement</p> <p>Per user subscription. Please contact sales@entersekt.com for more information.</p> <p>NICE Actimize; NuData Security</p> <p>3-D Secure ACS; transaction signing; mobile payments enablement platform</p> <p>Regional sales partners: Birger; Crealogix; CWG; Goodson Capital Partners; ICPS; MKTY; Netcetera</p>
Technology: Identity verification methods	
	Please email sales@entersekt.com for more information.
Authentication technology used	
	<p>Industry-standard X.509 digital certificates; proprietary validation techniques developed specifically for the mobile phone; FIPS 140-2 Level 3 on-premise hardware appliance; dynamic public key pinning; device and application context for context-based risk scoring; advanced detection of rooting, jailbreaking, or similar mobile operating system security bypass hacks; secure enablement of fingerprint, voice, iris biometrics; SIM-swap protection; NI USSD for non-app-based out-of-band authentication; FIDO authentication; secure browser pattern; behavioural analytics for real-time risk assessments; authentication orchestration</p>
Authentication Context	
	<p>Online Mobile ATM Branch POS Call centre</p>
<div>View company profile in online database</div>	

Reference Data connectivity	
Connectivity to governmental data	Please reach out to sales@entersekt.com for full details.
Other databases	Please reach out to sales@entersekt.com for full details.
Clients	
Main clients/references	Those listed in the public domain: Absa, Bayern Card-Services, Capitec Bank, Coutts, Discovery, Ecobank, Equifax, Equity Bank, FIS, FirstBank of Colorado, Investec, Nedbank, Old Mutual, Pluscard, Swisscard. For others, please contact our sales team.
Future developments	For more information, please contact our sales team.



Harness the power of trust.

Anything's possible when you partner with the best.

entersekt.com



Entersekt has always been mobile-first – we still are. We're proud to have pioneered phone-as-a-token out-of-band push authentication, which, over a decade later, has become the de facto market standard.

But fraud knows no limits, and that won't change. So, in support of true omnichannel experiences that match world-class security with superior user experience, we've expanded our focus to include two exciting new features.

NEW!



Browser authentication



Behavioral analytics

We also specialize in:



SCA for
PSD2



EMV
3-D Secure

Fraud
prevention



Customer
engagement



Reach out to us today to discuss how these features can help reduce your risk of fraud.

Email sales@entersekt.com or scan the code to visit our website.

Company	Fraugster
	<p>Fraugster is a fraud prevention company, which helps online merchants maximise their revenues while reducing operational costs. Fraugster serves clients across industries: from online retail and marketplaces to gaming and travel.</p> <p>Fraugster operates globally and serves merchants both directly and through payment companies, minimising the integration effort.</p>
Website Technology Target market Contact Geographical presence Year founded Service provider type - category Member of industry association and/or initiatives Company's motto	www.fraugster.com Native cloud Corporate Fintech Merchants/ecommerce PSP/acquirers SMBs sales@fraugster.com Worldwide 2014 Fraud platform Information available upon request Minimize Fraud. Maximize Revenue.
Services	
Unique selling points Pricing model Fraud prevention partners Other services Third party connection	<p>Fraugster provides fraud prevention services to online merchants both via direct integration and through partner PSPs, minimising the integration effort. We offer a variety of solutions: managed services, including chargeback protection and revenue increase guarantee, a self-service risk management suite (SaaS) as well as a hybrid model.</p> <p>Pricing is per transaction and based on volume and complexity OR SaaS-based pricing model</p> <p>Information available upon request</p> <p>N/A</p> <p>Ingenico ePayments, Ratepay, Worldline Six Payment solutions, CrefoPay</p>
Technology: Identity verification methods	
	Information available upon request
Authentication technology used	
	<p>Proprietary AI technology which combines human accuracy and machine scalability. We developed the Fraugster AI Engine based on a behavioural science approach that mimics the thought processes of a fraud analyst. Instead of clustering transactions, as done in classical machine learning, our technology analyses the behavioural context of each transaction, in order to accurately block fraudulent transactions while approving legitimate ones.</p> <p>Built on self-learning algorithms, the AI Engine detects and adapts to new fraud patterns as they emerge. Combined with a machine computation power, it processes thousands of transactions within milliseconds, enabling unlimited growth.</p>
Authentication Context	
	Online Mobile
Reference Data connectivity	
Connectivity to governmental data Other databases	N/A N/A
View company profile in online database	

Clients

Main clients/references

Ingenico ePayments, Six Worldline, Ratepay, Eurostep, AS Adventure, Diana SRL, European Games Group, Krefel, to name a few.

'Artificial Intelligence is the future of fraud prevention, and Fraugster's FraudFree helps our merchants improve their performance.' – Gabriel de Montessus, EVP Retail at Ingenico Group

'Fraugster's Fire is the perfect addition to our in-house machine learning platform. The flexible self-service rule engine allows our fraud analysts to quickly draft, test, and deploy anti-fraud rules directly into the real-time environment. Thanks to this cooperation, we can provide even greater customer experience to our merchants and their customers and help merchants drive revenue growth.' – Nicolas Kipp, Ratepay, Chief Risk Officer

'We chose Fraugster because it was the most sought out alternative to our previous solution. We said: let's give it a try, and now we couldn't be happier with the results. Our employee costs immediately went down once we eliminated manual reviews and our clients are now completely shielded from the trouble of chargeback costs.' – Giovanni Marconato, CFO – Problem Solver, Eurostep

Future developments

Information available upon request

NEVER WORRY ABOUT FRAUD AGAIN

Choose one or combine Fraugster's advanced AI fraud protection services

Managed service

chargeback protection and revenue increase, insured by Munich Re

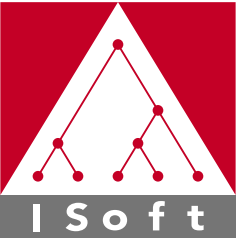
Powerful risk management suite

combining AI and custom rule writing, for risk teams

PSD2 solution

manage your transaction flow, raise exemptions and track performance

Minimize fraud. Maximize revenue.

Company	ISoft
	<p>ISoft is a leader in AI solutions for financial crime fighting. Our platform, based on real-time behavioural analysis and powered by machine learning, has been chosen by 4 of the Top 10 European banks for its ability to detect and stop threats accurately while reducing customer friction.</p>
<p>Website</p> <p>Technology</p> <p>Target market</p> <p>Contact</p> <p>Geographical presence</p> <p>Year founded</p> <p>Service provider type - category</p> <p>Member of industry association and/or initiatives</p> <p>Company's motto</p>	<p>www.isoft.fr</p> <p>On-premises Cloud enabled Native cloud Hybrid</p> <p>Retail banks Digital banks/fintechs Issuing banks Acquiring banks Financial institutions Payment services providers Ecommerce merchants Governments/enterprises</p> <p>contact@isoft.fr</p> <p>Global</p> <p>1990</p> <p>Fraud platform Consumer authentication Merchant risk/Transaction laundering prevention Digital identity service provider Technology vendor Web fraud detection company</p> <p>Information available upon request</p> <p>N/A</p>
Services	
<p>Unique selling points</p> <p>Pricing model</p> <p>Fraud prevention partners</p> <p>Other services</p> <p>Third party connection</p>	<p>ISoft is a European leader in AI solutions for financial crime fighting. We provide the most complete and fastest AI platform for real-time threat detection and immediate response to new fraud patterns. ISoft protects more than EUR 40 billion every day.</p> <p>Information available upon request</p> <p>Information available upon request</p> <p>Customer specific fraud fighting modelling, fraud strategy audit, professional services</p> <p>Several third-party API connections</p>
Technology: Identity verification methods	
	<p>Real-time transactions evaluation, fraud detection machine learning models, behavioural analysis, data science platform, payer authentication, device fingerprint, velocity rules – purchase limit rules, link analysis, geo-location checks, BIN lookup, white list/blacklist, KYC, follow-up action, case management</p>
Authentication technology used	
	<p>ISoft solution drives the authentication strategy required by PSD2 (Real-Time Risk Based Analysis). We partner with main authentication market solutions.</p>
<div data-bbox="1066 2040 1522 2085">View company profile in online database</div>	

Authentication Context	
	Omnichannel ATM Point-of-sale Online banking Mobile Call centre
Reference Data connectivity	
Connectivity to governmental data	Information available upon request
Other databases	Our APIs enable connection with the main providers of the market.
Clients	
Main clients/references	4 of the Top 10 largest European banks and more than EUR 40 billion protected every day
Future developments	Information available upon request



ISoft

LEADER AI-BASED PLATFORM FOR FINANCIAL CRIME FIGHTING

UNPARALLELED REAL-TIME THREAT PREVENTION
ENHANCED CUSTOMER EXPERIENCE

+40 BILLION EUROS

Scored in Real-Time each day


4 OF TOP 10

European Banks

+40 MILLION PEOPLE

Protected

ISoft's omnichannel Risk Management solutions are based on the fastest and most complete AI Technology for **threat detection in Real-Time** and **immediate response to new fraud patterns**.

Company	Kount
	<p>Kount's Identity Trust Global Network delivers real-time fraud prevention and account protection, and enables personalised customer experiences for more than 9,000 leading brands and payment providers. Linked by Kount's award-winning AI, the Identity Trust Global Network analyses signals from 32 billion annual interactions to personalise user experiences across the spectrum of trust — from frictionless experiences to blocking fraud. Quick and accurate identity trust decisions deliver safe payment, account creation, and login events while reducing digital fraud, chargebacks, false positives, and manual reviews.</p>
<p>Website</p> <p>Technology</p> <p>Target market</p> <p>Contact</p> <p>Geographical presence</p> <p>Year founded</p> <p>Service provider type - category</p> <p>Member of industry association and/or initiatives</p> <p>Company's motto</p>	<p>www.kount.com</p> <p>Cloud enabled Native cloud Hybrid</p> <p>Banks/FS Corporate Fintech Merchants/ecommerce PSP/acquirers SMBs Telecom</p> <p>kount.com, info@kount.com</p> <p>Global</p> <p>2007</p> <p>Fraud platform Data provider and verification Chargeback management Merchant risk/Transaction laundering prevention</p> <p>Merchant Risk Council, National Retail Federation, CPE Credit Certification by NASBA, Internet Merchants Retail Group, Global Retail Insights Network</p> <p>Protecting your digital innovation</p>
Services	
<p>Unique selling points</p> <p>Pricing model</p> <p>Fraud prevention partners</p> <p>Other services</p> <p>Third party connection</p>	<p>Kount's solution leverages its Identity Trust Platform to enable digital businesses to screen for multiple fraud use cases including payments, digital accounts, bots, friendly fraud, mobile, loyalty, eGift card, and more.</p> <p>Kount has different pricing models by use case and desired services.</p> <p>https://kount.com/partners including Barclays, Chase, Moneris, Braintree, BlueSnap, and 50+ more</p> <p>Account takeover protection, new account creation protection, data on demand, criminal and friendly fraud prevention, managed services, CB guarantee, advanced analytics, VMPI, training & support</p> <p>Several third-party API connections</p>
Technology: Identity verification methods	
	Transaction verification, email verification, address verification, phone verification
Authentication technology used	
	Device fingerprinting, geo-location, remote access detection, 3-D Secure 2.0, remote access detection
Authentication Context	
	Online Mobile
<div>View company profile in online database</div>	

Reference Data connectivity	
Connectivity to governmental data	N/A
Other databases	Ekata, Ethoca, LexisNexis, Neustar
Clients	
Main clients/references	9,000+ brands globally, including Staples, PetSmart, Dunkin, GNC, Fetch Rewards, Conair, JoAnn Fabrics, and many more
Future developments	Kount is continuously delivering net new functionality month after month, contact info@kount.com for more information.

AI-Driven

Identity Trust Platform

Powered by Identity Trust Global Network™

Account
Takeover &
Bot Protection


eCommerce
Fraud
Prevention

Chargeback
Prevention

Industry-leading fraud protection for the entire customer journey. Reduce chargebacks, manual reviews, and false positives to increase approval rates and revenues.



+1 (866) 442-2659 | info@kount.com | www.kount.com

Company	Netcetera
	<p>As market leader for 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>
<p>Website</p> <p>Technology</p> <p>Target market</p> <p>Contact</p> <p>Geographical presence</p> <p>Year founded</p> <p>Service provider type - category</p> <p>Member of industry association and/or initiatives</p> <p>Company's motto</p>	<p>www.netcetera.com</p> <p>On-premises Cloud enabled Native cloud</p> <p>Banks/FS Fintech Merchants/ecommerce PSP/acquirers</p> <p>info@netcetera.com</p> <p>Europe, Middle East, APAC, Africa, Americas</p> <p>1996</p> <p>Consumer authentication</p> <p>EMVCo, Mobey Forum</p> <p>We interconnect the payment ecosystem to deliver a trusted digital payment experience.</p>
Services	
<p>Unique selling points</p> <p>Pricing model</p> <p>Fraud prevention partners</p> <p>Other services</p> <p>Third party connection</p>	<p>Netcetera delivers an outstanding 3DS service, fully tailored to the individual needs of issuers, acquirers, PSPs, and merchants. Being an EMVCo technical associate we are actively shaping the future of secure and seamless payments with an end-to-end view.</p> <p>Pricing is per transaction and based on volume and complexity or SaaS-based pricing model.</p> <p>Risk assesment platforms like Riskshield from Inform</p> <p>White label banking, card management, wallet apps, tokenization, authentication solutions</p> <p>Partners are market and solution specific; information on request.</p>
Technology: Identity verification methods	
	<p>Netcetera supports all identity verification methods used by card issuers and can connect to third-party ID provider systems.</p>
Authentication technology used	
	<p>Netcetera uses PSD2 compliant Strong Customer Authentication based on device binding, biometric technologies, risk assessment using machine learning. In addition, we offer exemption advise, tokenization and delegated authentication technologies as well as mobile SDKs for 3DS and mobile card management apps. We support all EMV 3DS standards, FIDO, Open Authentication, and many more. Our solutions are certified by EMVCo, Mastercard, Visa, and other major schemes.</p> <p>EMV and 3-D Secure are registered trademark from EMVCo.</p>
Authentication Context	
	<p>In our 3DS 2.x services we authenticate ecommerce transactions.</p> <p>In our mobile wallet offering we authenticate payment transactions on the smartphone for POS usage as well as push-based authentication for ecommerce payments.</p>
Reference Data connectivity	
<p>Connectivity to governmental data</p> <p>Other databases</p>	<p>N/A</p> <p>N/A</p>
View company profile in online database	

Clients

Main clients/references

Most of the leading banks from Germany, Austria, and Switzerland rely on Netcetera 3DS services. Please visit our website www.netcetera.com for references and customer testimonials.

Future developments


Merchant Network Tokenization, Click To Pay, Delegated Authentication, PSD2 Exemption Advisor

netcetera

Secure Digital Payments



www.netcetera.com

Company	
Nok Nok Labs, Inc.	
	<p>Nok Nok provides secure, scalable, and frictionless experiences for passwordless authentication, preventing fraud and security risks. By reducing the reliance on weak, phishable passwords, Nok Nok empowers organisations to improve the authentication experience, while meeting the most advanced security and regulatory requirements. Customers include cloud, mobile, and IoT businesses.</p>
Website Technology Target market Contact Geographical presence Year founded Service provider type - category Member of industry association and/or initiatives Company's motto	<p>www.noknok.com</p> <p>On-premises Cloud enabled Hybrid</p> <p>Banks/FS Corporate Fintech Merchants/ecommerce PSP/acquirers SMBs Telecom</p> <p>Walter Beisheim: wbeisheim@noknok.com</p> <p>Global</p> <p>2011</p> <p>Fraud platform Consumer authentication ID verification Data provider and verification Chargeback management Merchant risk/Transaction laundering prevention</p> <p>The FIDO Alliance, MRC, GSMA</p> <p>Know Who's There</p>
Services	
Unique selling points Pricing model Fraud prevention partners Other services Third party connection	<p>Nok Nok reduces the reliance on passwords and other broken legacy authentication methods with a scalable platform that easily integrates into existing security environments. An inventor of FIDO, our platform sets the standard for compliant deployments. Nok Nok leads in deployments and innovation, driving adoption, and expanding use cases.</p> <p>Per user annual subscription</p> <p>Aware, DDS, Forgerock, Fujitsu, Hitachi, iLabs, Jumio, Lenovo, Mtrix, NTT Data, OneSpan, OSD, Sensory, Younixq, Yubico</p> <p>Professional Services to guide an organisation to completely passwordless authentication. We assess authentication architecture, build an understanding of problems, needs, and desires. We map the ecosystem of technology partners and providers locating the strengths and weaknesses in order to leverage strengths and minimise weaknesses. We introduce a solution framework to provide the understanding of the technology, the trade-offs, future considerations, and expected benefits.</p> <p>N/A</p>
Technology: Identity verification methods	
	<p>Identity document scanning, video scanning, email verification, phone verification, behavioural biometrics, physical biometrics, device fingerprinting, geo-location, mobile app push, 3-D Secure 2.0, one-time passwords, hardware token</p>
Authentication technology used	
	<p>Public/private encryption key matching, behavioural biometrics, physical biometrics, device fingerprinting, geo-location, mobile app push, 3-D Secure 2.0, hardware token, one-time passwords</p>
View company profile in online database	

Authentication Context	
	Online Mobile ATM Call center
Reference Data connectivity	
Connectivity to governmental data	N/A
Other databases	N/A
Clients	
Main clients/references	NTT DOCOMO, T-Mobile, BBVA, Intuit, Standard Bank, MUFG, Softbank, Gallagher, and more
Future developments	Information available upon request

Passwordless Authentication


Frictionless Experiences
for Connected Customers

Millions of people, applications and devices rely on Nok Nok's passwordless authentication solutions. That's because Nok Nok has solved the connected customer authentication problem—so you ***Know Who's There.***

www.noknok.com



**nok
nok**
Know Who's There

Company	SecuredTouch
 SECUREDTOUCH	<p>SecuredTouch provides real-time, adaptive fraud detection throughout the customer journey to detect fraud early, with proven ROI from day 1. Our solution ensures accurate risk-based prevention for multiple use cases including ATO, bots, and no-transaction fraud. SecuredTouch customers benefit from reduced overall fraud losses while maintaining a smooth customer experience.</p>
Website	www.securedtouch.com
Technology	Cloud enabled Native cloud Hybrid
Target market	Banks/FS Fintech Merchants/ecommerce PSP/acquirers Telecom
Contact	lior@securedtouch.com
Geographical presence	US, EMEA
Year founded	2014
Service provider type - category	Fraud platform Consumer authentication Merchant risk/Transaction laundering prevention
Member of industry association and/or initiatives	MRC
Company's motto	Adaptive fraud detection throughout the customer journey
Services	
Unique selling points	<p>SecuredTouch provides visibility into the entire customer journey to uncover behavioural anomalies and non-human behaviours, and detect fraud at any stage, before checkout, even when no transaction takes place.</p> <p>Its monitoring and analytics capabilities adapt to your specific business use cases and provide zero-day detection for unknown threats.</p>
Pricing model	Based on session volume
Fraud prevention partners	ForgeRock, Arvato
Other services	N/A
Third party connection	ForgeRock
Technology: Identity verification methods	
	Main fraud use cases: Account takeover; Tools detection (bots, emulators, device anomalies); New account fraud; Payment/checkout fraud.
Authentication technology used	
	Behavioural anomalies (navigation patterns, application fluency, data familiarity, user journey) Behavioural biometrics (keystrokes and B28, touchscreen and mobile sensors) Device intelligence (device fingerprinting, tampered/spoofed devices, emulators, cloning apps) Network analysis (IP analysis, data centers/hosting, network/carrier/ISPs etc.) Velocity checks
Authentication Context	
	Online (desktop & mobile) Mobile (Native applications for both android & iOS)
View company profile in online database	

Reference Data connectivity	
Connectivity to governmental data	N/A
Other databases	N/A
Clients	
Main clients/references	Trusted by top global merchants, including Wish.com, Gett & MIT.
Future developments	<p>An offering for banks</p> <p>Addition of deep learning and semi-supervised machine learning modules to the platform</p> <p>Application of insights and patterns across clients (from one merchant to another)</p> <p>Adding visibility into the fraudster's journey and expose relevant business vulnerabilities</p>



PREVENT FRAUD AT ANY TIME IN THE CUSTOMER JOURNEY

SecuredTouch has developed an adaptable zero-day approach that detects fraud early before a transaction can take place. A single platform supports multiple use cases, with measurable ROI from day 1.



ACCOUNT TAKEOVER DETECTION

Flag illegitimate access of your customer's accounts regardless of the attack vector



PAYMENT FRAUD DETECTION

Identify behavioral anomalies to catch the purchase of goods and services using stolen credit card details




BOT DETECTION


Separate human from non-human behaviors to prevent credential stuffing, sneaker bots and more with a frictionless solution



NO-TRANSACTION FRAUD DETECTION

Monitor the customer journey to stop refund, referral, coupon and loyalty fraud and more

Company	SEON Technologies Ltd.
	<p>SEON reduces risk and boosts conversions for highly targeted verticals such as banking, lending, FX, crypto trading, iGaming, and ecommerce. SEON's innovative tools let you decide how you integrate fraud prevention into your platform, either as individual modules for multi-layered security, or as a whole end-to-end system.</p>
<p>Website</p> <p>Technology</p> <p>Target market</p> <p>Contact</p> <p>Geographical presence</p> <p>Year founded</p> <p>Service provider type - category</p> <p>Member of industry association and/or initiatives</p> <p>Company's motto</p>	<p>seon.io</p> <p>On-premises Cloud enabled Native cloud Hybrid</p> <p>Banks/FS Fintech Merchants/ecommerce PSPs/acquirers Travel iGaming Online lending FX eSports SMBs Telecom</p> <p>info@seon.io Phone: +44 20 8089 2900</p> <p>Global</p> <p>2017</p> <p>Fraud platform Digital identity Email analysis Phone analysis Device fingerprinting Consumer authentication ID verification Data provider and verification Chargeback management Merchant risk/Transaction laundering prevention</p> <p>N/A</p> <p>Fraud fighting done differently</p>
Services	
<p>Unique selling points</p> <p>Pricing model</p> <p>Fraud prevention partners</p> <p>Other services</p> <p>Third party connection</p>	<p>At SEON, we believe you need three things to reduce fraud and grow your business with complete peace of mind: access to better data, complete integration and implementation flexibility, and full transparency in how the products and the company works.</p> <p>Pricing is per transaction and based on volume and complexity or SaaS-based pricing model.</p> <p>N/A</p> <p>N/A</p> <p>N/A</p>
<div data-bbox="1066 2040 1522 2085">View company profile in online database</div>	

Company	Sift
	<p>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 35 billion events per month, and a commitment to long-term customer partnerships.</p>
<p>Website</p> <p>Technology</p> <p>Target market</p> <p>Contact</p> <p>Geographical presence</p> <p>Year founded</p> <p>Service provider type - category</p> <p>Member of industry association and/or initiatives</p> <p>Company's motto</p>	<p>www.sift.com</p> <p>Native cloud</p> <p>Cloud enabled</p> <p>Digital and physical ecommerce</p> <p>Fintech</p> <p>Cryptocurrency</p> <p>Payment services providers</p> <p>Online communities/web merchants</p> <p>Gaming & gambling</p> <p>Travel</p> <p>On-demand services</p> <p>Online ticketing</p> <p>Marketplaces</p> <p>QSRs (Quick Serve Restaurants)</p> <p>Fast casual restaurants</p> <p>sales@sift.com</p> <p>Global</p> <p>2011</p> <p>Fraud platform</p> <p>Merchant Risk Council (MRC), Merchant Advisory Group (MAG)</p> <p>Help everyone trust the internet</p>
Services	
<p>Unique selling points</p> <p>Pricing model</p> <p>Fraud prevention partners</p> <p>Other services</p> <p>Third party connection</p>	<p>Live machine learning, global network, and advanced automation</p> <p>Pay as you go with volume discounts based on transaction volume</p> <p>Ekata, Chargeback Gurus, Chargebacks911, Midigator, Chargeback.com, Arvato, CES</p> <p>Integration and support</p> <p>Salesforce Commerce Cloud, Adobe Magento, Shopify, Olo, Dwolla</p>
Technology: Identity verification methods	
	<p>Address verification services, CNP transactions, BIN lookup, geo-location checks, device fingerprint, chargeback reduction, velocity rules, white list/black list database, KYC, behavioural analysis, two-factor authentication, machine learning, data analytics, follow-up action</p> <p>More information available upon request</p>
Authentication technology used	
	<p>Sift offers multi-factor authentication but is not an identity access manager. However, Sift's solution can integrate signals from authentication vendors such as biometrics into our risk assessments.</p>
Authentication Context	
	<p>Online</p> <p>Mobile</p>
Reference Data connectivity	
<p>Connectivity to governmental data</p> <p>Other databases</p>	<p>N/A</p> <p>Multiple</p>
View company profile in online database	

Clients

Main clients/references	Airbnb, Boltpay, Box, Cabify, Carousell, ChowNow, Destinia, Doordash, Everlane, Fitbit, GetYourGuide, Glassdoor, Harry's, HelloFresh, Hopper, Indeed, Instacoins, Kamernet, Logitravel, Patreon, Poshmark, Pushpay, Rapyd, Reddit, Ritual, SendCloud, Shutterstock, Startselect, Traveloka, Turo, Twilio, Twitter, Unity, Upwork, Viagogo, Wayfair, Yelp, Zillow
Future developments	Expanding products and markets

Online fraud stops here.

Sift's Digital Trust & Safety Suite is the only fraud prevention solution that puts your business at the intersection of protection and growth—so you can align risk and revenue decisions, and fight fraud without losing customers, money, or momentum.



Drive expansion without burning resources, and continuously improve risk mitigation strategies with in-depth reporting and data transparency.

Features like Dynamic Friction and Insult Monitor reduce false positives, allowing trusted customers to face less friction and frustration whenever they interact with your site.



With real-time machine learning and actionable feedback, your fraud prevention strategy gets smarter by the minute—and you stop fraudsters no matter where or how they attack.



Visit sift.com today to start your Digital Trust & Safety transformation.

Over 34,000 sites and apps trust Sift to deliver outstanding customer experiences while preventing fraud and abuse.



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.
Website Technology Target market Contact Geographical presence Year founded Service provider type - category Member of industry association and/or initiatives Company's motto	www.signifyd.com Native cloud Merchants/ecommerce Ashley Kiolbasa, Head of Product Marketing @ Signifyd; ashley.kiolbasa@signifyd.com Global 2011 Fraud platform Consumer authentication ID verification Chargeback management MRC, British Retail Consortium One end-to-end platform for fearless commerce
Services	
Unique selling points Pricing model Fraud prevention partners Other services Third party connection	Signifyd is the largest provider of commerce protection with a network of over 10,000+ merchants. Signifyd optimises merchants' revenue with a unique combination of big data, machine learning, and domain expertise to address all chargeback types and to ensure that legitimate orders are not wrongly declined. We demonstrate our trust in our decisions with a 100% financial guarantee for approved orders that result in fraud or item-not-received chargebacks. Pricing model varies Accertify, CyberSource 3DS 2.2 + Certified vendor Accertify, BigCommerce, Cybersource, Magento, NetSuite, Salesforce, SAP, Shopify, PayPal, Braintree, Clientline, ChasePaymentech, Adyen, Stripe
Technology: Identity verification methods	
	With a global network of over 10,000+ merchants in 100+ countries, Signifyd can identify 98% of consumers based on one or more of the following variables: email address, IP address, phone number, physical address, and device ID. Additionally, Signifyd leverages behavioural data, proxy detection, social graph data, purchasing history, issuing bank data, cross merchant blacklists, transaction velocity, search engines, and public records to further verify consumer identity.
Authentication technology used	
	Signifyd's Payments Compliant solution, Seamless SCA gathers device token information, behavioural metrics, and biometric data to authenticate the consumer as they shop – before they even reach check out. Built in 3-D Secure 2.2 functionality dynamically links payment to the issuing banks and confirms that SCA has been conducted.
Authentication Context	
	Online
Reference Data connectivity	
Connectivity to governmental data Other databases	Public records/publicly available government data In addition to a global network of over 10,000+ merchants, Signifyd also pulls in data from public databases and industry-standard data vendors.
View company profile in online database	

Clients

Main clients/references

Emma Mattress, Illy, Lacoste, Omega, Mango, Lego, Samsung, Reckitt Benckiser

Future developments

More information upon request

Embrace Fearless Commerce

Signifyd provides the most seamless and scalable approach to commerce protection for enterprise retailers. By leveraging the power of the largest commerce network available today, Signifyd effortlessly automates customer experience, maximizes conversion and frees merchants to embrace a world without fraud and abuse.



Payments Compliance

Seamless authentication and PSD2 compliance, guaranteed.



Revenue Protection

Liability shift and 4 - 6% revenue lift.



Abuse Prevention

Protection from unwanted policy abuse by customers.

Trusted by Leading
Enterprises Globally

SAMSUNG

GUINNESS

illy

RITE AID

LACOSTE

LEGO

Moosejaw

emma

OMEGA

build.com


Reckitt
Benckiser

MANGO

 SIGNIFYD

www.signifyd.com



Company		Simility, a PayPal Service	
		Simility offers real-time fraud and risk decisioning solutions to protect global businesses. Simility's Adaptive Decisioning Platform is built with a data-first approach to deliver continuous risk assurance. By combining advanced machine learning and big data analytics, Simility helps businesses orchestrate decisions to reduce friction, improve trust, and solve complex fraud problems.	
Website		https://simility.com/	
Technology		SaaS On-premises Virtual private cloud (VPC) models	
Target market		Large ecommerce merchants Financial institutions Fintechs	
Contact		contact@simility.com	
Geographical presence		Global coverage with offices in San Jose (US), Hyderabad (India), London (UK), Amsterdam (NL), and Sao Paulo (Brazil)	
Year founded		2014	
Service provider type - category		Technology vendor Web fraud detection company	
Member of industry association and/or initiatives		MRC	
Company's motto		The end-to-end fraud decisioning platform	
Services			
Unique selling points		Complete enterprise fraud management platform, with: Ingress Processing, Device Recon, Third Party Validation, Advanced Analytics, White-box Machine Learning, Champion Challenger, AutoML, Intuitive Rule Builder, Automatic Rule and Threshold Recommendations, Rule Simulation, Robust Link Analysis, Case Management, Workbench, PayPal two-sided network intelligence	
Pricing model		Per-transaction and on-premise license pricing models, professional services pricing information available upon request	
Fraud prevention partners		Equifax, HCL Technologies	
Other services		Data science as a service, historical data analysis	
Third party connection		Simility can connect to various third-party feeds, including internal customer data feeds.	
Technology: Identity verification methods			
		Personally identifiable information (PII) validation, small transaction verification, email verification, phone verification, social verification, credit check, compliance check	
Authentication technology used			
		Password/phrase, one-time password, multi-factor authentication, device fingerprinting, geo-location, remote access detection	
Authentication Context			
		Online Mobile ATM POS Call centre Other – branch banking data	
Reference Data connectivity			
Connectivity to governmental data		More information available upon request	
Other databases		Variety of third-party services	
<div>View company profile in online database</div>			
FRAUD PREVENTION IN ECOMMERCE REPORT 2020 / 2021 COMPANY PROFILES			

Clients

Main clients/references

Customers include Global 500 in financial services, ecommerce, payments, classifieds.
Public references include US Bank, Chime, Jumia, OfferUp, Luisaviaroma, Zions Bank.

Future developments

Machine learning enhancements, advanced rule management, advanced integration with Braintree, granular access control

Transforming the way businesses detect fraud

Tailored, end-to-end solutions that help
provide real-time fraud intelligence

Reduce Fraud Losses

Enhance Customer Experience

Detect Emerging Fraud Threats

Leverage Best-in-Class Machine Learning & Analytics

GET STARTED TODAY

An AI-based Fraud Prevention and Risk Management Platform
That Continuously Adapts As Fraud Evolves.

[SIMILITY.COM/DEMO](https://similarity.com/demo)



simility
A **PayPal** Service

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

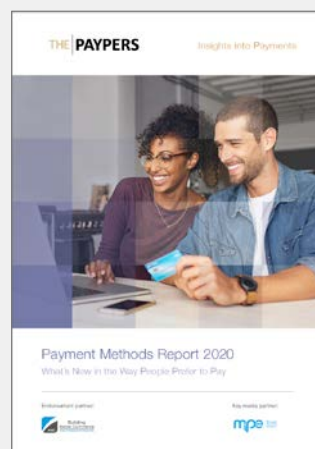
Once a year, The Paypers releases four large-scale industry overviews covering the latest trends, developments, disruptive innovations and challenges that define the global online/mobile payments, e-invoicing, B2B payments, ecommerce and web fraud prevention & digital identity space. Industry consultants, policy makers, service providers, 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.



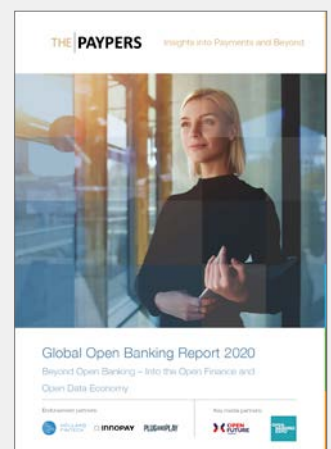
**Who's Who in
Payments 2020**



**Digital Onboarding
and KYC Report 2020**



**Payment Methods
Report 2020**



**Global Open Banking
Report 2020**

For the latest edition, please check the Reports section

