callsign

THREATS SERIES

WHITEPAPER

Fraud prevention for merchant businesses

Seamless and secure digital identification that preserves trust and streamlines customer journeys

OVERVIEW

Doing business in a digital world

If shopping online wasn't already second nature for consumers, it certainly is now – even for older consumers

Paypal recently revealed that its fastest-growing demographic – globally – is people over 50 years old.[1] A 2020 report[2] estimates that 17.2 million Brits plan to continue shopping online permanently, including those older generations. In western Europe, McKinsey research shows that between 60 to 85% of consumers[3] now prefer to make everyday transactions digitally, including those who are 65 and older. And in the US, nearly half (47%) of Baby Boomers – who have historically been less likely to buy online – Also plan to increase their online shopping, even after the pandemic.[4]

For merchants, the opportunity is clear: more customers, more sales, and more profit. But as the market gets bigger, so does the risk. With every transaction, the threat of fraud rears its head – and the pressures faced by merchants grow more complex day by day.

External challenges, internal pressures

Merchants navigate a landscape of labyrinthine complexity. In a world where cyber attacks and social engineering are rife and data breaches are quickly followed by bots mass testing credentials, bad actors are using increasingly sophisticated methods to gain access to data. The risk of high chargebacks, damaged reputations, and lost customers are omnipresent. Bad actors are also getting better at overcoming existing fraud prevention measures, meaning tried-and-trusted lines of defense are crumbling with greater regularity.

Yet even as the urgency for greater security grows, there's a need to avoid compromising user experience (UX) for shoppers across multiple channels. Convenience and ease are primary drivers for online shopping, and with the rise of omnichannel retail, shoppers can truly buy 'anywhere, anytime'. But if it takes too long to log in or complete a purchase, customers will go elsewhere. YouGov research for Callsign[5] showed that in April 2020 alone, 20% of consumers switched to other brands due to a bad online shopping experience, such as failed payments or overcomplicated logins.

Consumers demand friction-free experiences across every channel; but they also expect rigorous account security. Fraudsters are acting with increasing sophistication, and their nets are growing larger. And no matter where they're based, if a business sells to European customers, it must comply with GDPR, along with other regulations.

So how can merchants square this security circle – especially considering the huge array of challenges that exist both within and outside the organization?

[1] ***PayPal reports surge in usage:*** *https://micky.com.au/paypal-reports-surge-in-usage-from-people-of-50/*

[2] ***The impact of COVID-19 on the retail industry:*** *https://www.alvarezandmarsal.com/insights/impact-covid-19-uk-retail-industry*

[3] ***Reshaping retail banking for the next normal:*** *https://www.mckinsey.com/industries/financial-services/our-insights/reshaping-retail-banking-for-the-next-normal#*

[4] ***New research shows baby boomers will continue shopping online post-pandemic:*** *https://lasership.com/whitepaper_2020.php*

[5] ***Impact of 2020 pandemic:*** *https://blog.callsign.com/impact-of-2020-pandemic-report*

SECTION TWO

Understanding the threat:
What merchants are up against

To find a comprehensive solution, merchants must be sure to understand the nuances of the threats in the field – which is no mean feat, considering these risks are continually evolving.

In a recent study by Worldpay,[6] merchants stated that the most common types of eCommerce fraud causing them concern were identity theft (71%), phishing (66%) and account theft (63%). While increasingly sophisticated attacks are hard to combat, understanding the different ways that bad actors operate is the first step to finding a solution that could address them all.

[6] ***KPMG Global Banking Fraud Survey 2019:*** *https://home.kpmg/xx/en/home/insights/2019/05/the-multi-faceted-threat-of-fraud-are-banks-up-to-the-challenge-fs.html*

Account opening

On the quest to offer the most seamless experiences possible, merchants may reduce authentication and verification requirements, increasing the risk of account opening fraud (also known as new account fraud or online account origination fraud).

This is a particular concern for businesses that offer sign-up bonuses and new customer discounts. Fraudsters use stolen or synthetic identities to open new shopping accounts. Using 'real' details in this manner means that fraudulent applications may no be detected until weeks after an account is opened.

Attempts may include:

Synthetic IDs: Identities created by combining personal details of more than one person. These identities can then be used to make purchases through merchant sites, often racking up large bills.

Impersonation: Incorporating genuine but falsely-obtained information taken from documents such as passports, national identity documents, and correspondence; data stripped from open sources such as social networking sites; or birth and death registers. Data can also be harvested from social engineering scams.

Multiple applications: Bad actors create seemingly legitimate firms, and use these to open several accounts with different synthetic identities at once. By creating interactions between the different IDs, scammers can bolster each account's credit score, helping build the illusion of authenticity.

Friendly fraud: When a consumer makes a purchase using their own credit card, then requests a chargeback after receiving the goods or services. Because this type of fraud is initiated by a genuine account holder, it's difficult to spot.

Account borrowing: Users allowing bad actors, family, or friends to use their accounts. Without the appropriate security measures in place, this is hard to detect, as the user has deliberately given their identity or personal information to another.

Account takeover (ATO)

Many account takeovers originate from data breaches, often refined and sold on the dark web, either individually or in aggregate. ATOs may also stem from phishing emails or social engineering. Regardless of approach, criminals / scammers obtain the data they need to mimic a user's identity and infiltrate customer accounts to take control. No merchant wants to allow bad actors to take control of genuine customer accounts – but those offering loyalty points or vouchers

may be even more at risk, as fraudsters know these can easily be swapped for products or even cash.

Methods of ATO can include:

Credential stuffing: Either manually or through automation, malicious actors systematically test stolen credentials from data breaches across a range of sites. This is a subset of the brute force attack. Known username/password pairs are entered into huge numbers of websites to find matches with real user accounts.

Scripted attacks: Large-scale, organized attacks – normally automated by bots – that scrape user data and inventory. Customized bots use programming scripts to select specific products from online stores and buy them at inhuman speed.

Identity fraud

Identity fraud or theft involves a bad actor using the victim's personal information to open shopping or bank accounts. Identity theft often involves social engineering, where the fraudster impersonates trusted figures such as a bank, a government agency, or a much-used shopping site. Victims are manipulated into revealing personal or financial data, such as a password or PIN.

Man-in-the-middle attacks see supposedly secure communications intercepted: To steal login credentials or personal information, spy on the victim, sabotage communications, or corrupt data.

Merchants that offer credit are particularly susceptible to this, as they don't necessarily have the capabilities to run proper checks or robust identity verification processes in addition to credit score checks.

Payment fraud

Payment fraud involves a bad actor stealing details of a credit or debit card, or a bank account, and making unauthorized purchases.

These purchases are often sold on quickly for cash.

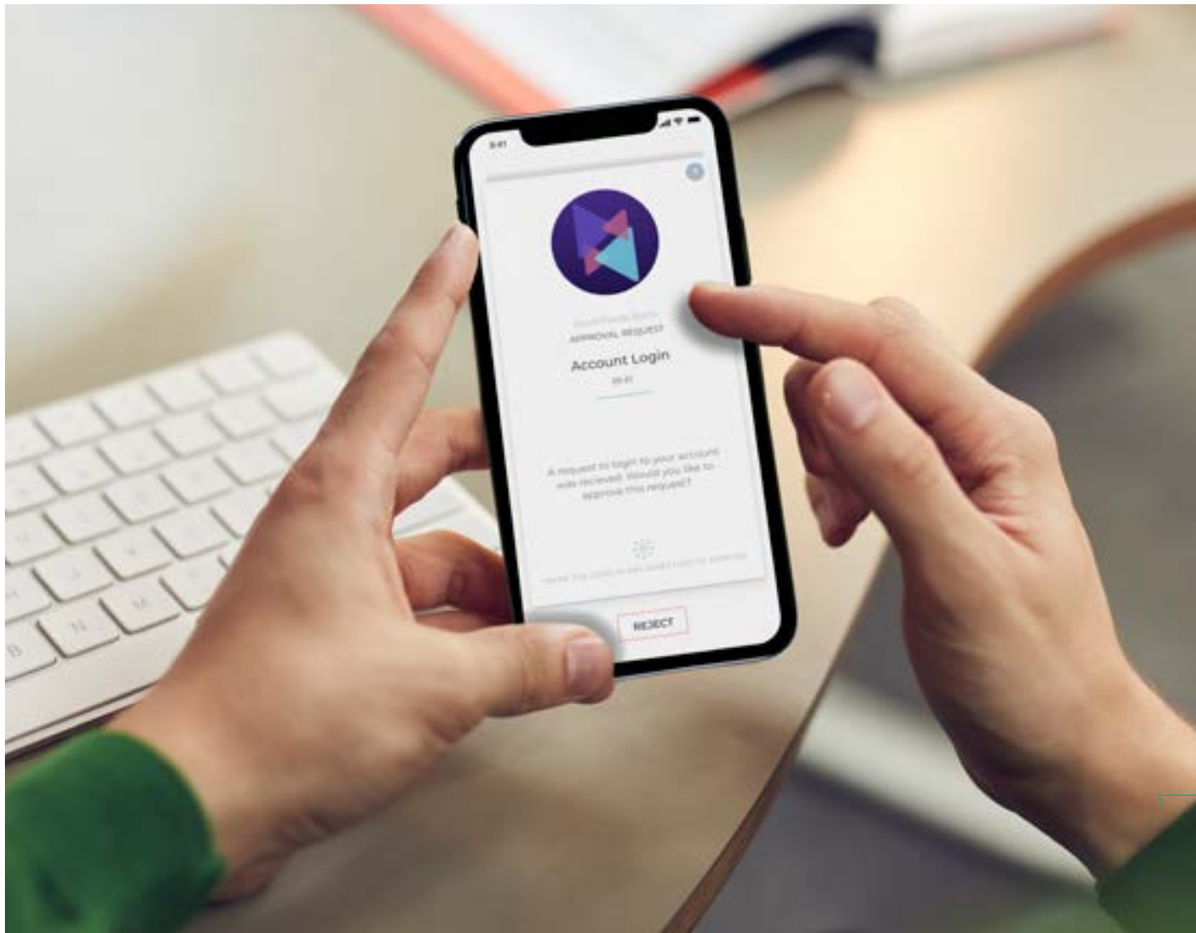
This is a serious issue for merchants, as while customers may be able to claim unauthorized spending back from their bank, the distress and inconvenience could mean a loss of trust in your business. Merchants with a card on file capability must be particularly careful. And while compliance with regulations (such as PSD2 in Europe) should help to lessen this fraud, it shouldn't be at the expense of customer experience, which could be equally damaging for merchants.

An intelligent solution

Whatever the type of fraud, merchants must be on their guard. The consequences of failing to protect customer data adequately can be severe; identity theft, for example, can affect the victim's credit score and cause significant personal problems. And, once discovered, it can take months or years to undo the damage.

A data breach that makes customer details vulnerable could cause long-term costs, reputational damage, and even the total breakdown of a merchant business.

Accordingly, with threats varied and ever-evolving, the value of intelligent fraud prevention is clear. But for merchants striving to make sales and capture new customers, any fraud solution must harmonize with another goal: that of seamless customer experience.



SECTION THREE

Balancing security with customer experience

Merchants and customers alike can agree to the importance of fraud prevention

Implementing robust security is vitally important; but it has to be weighed up against user experience and accessibility. If security protocols disrupt customer journeys (or even hinder employees while working), the friction produced can cause real problems for customers and merchants alike. It's a fine balance.

It's well-reported that shoppers value ease. Research by the Aberdeen Research Group from 2008 has shown that mobile sites lose 7% of their customers for every second they take to load.[7] An exasperating user experience can quickly lead to abandoned carts, frustrated shoppers, and long-term loss of customers – meaning that an approach to security that produces a lot of false positives can be more costly than the fraud you're trying to prevent. If you turn a real customer away, you may lose them forever; a particularly concerning point, considering a PwC survey[8] found 34% of respondents thought their organization's use of technology to combat fraud was producing too many false positives.

For merchants, making sure you let in every 'good' transaction is just as important as keeping out the 'bad' ones. The answer is finding the right balance between experience and security for each organization – or ideally, for each transaction.
And this will only grow more important as merchants strive to move toward one-click payments, as pioneered by the likes of Amazon. This offers the ultimate in UX and reduces abandoned transactions for merchants, but in order for customers to trust this as a payment method, robust security is vital.

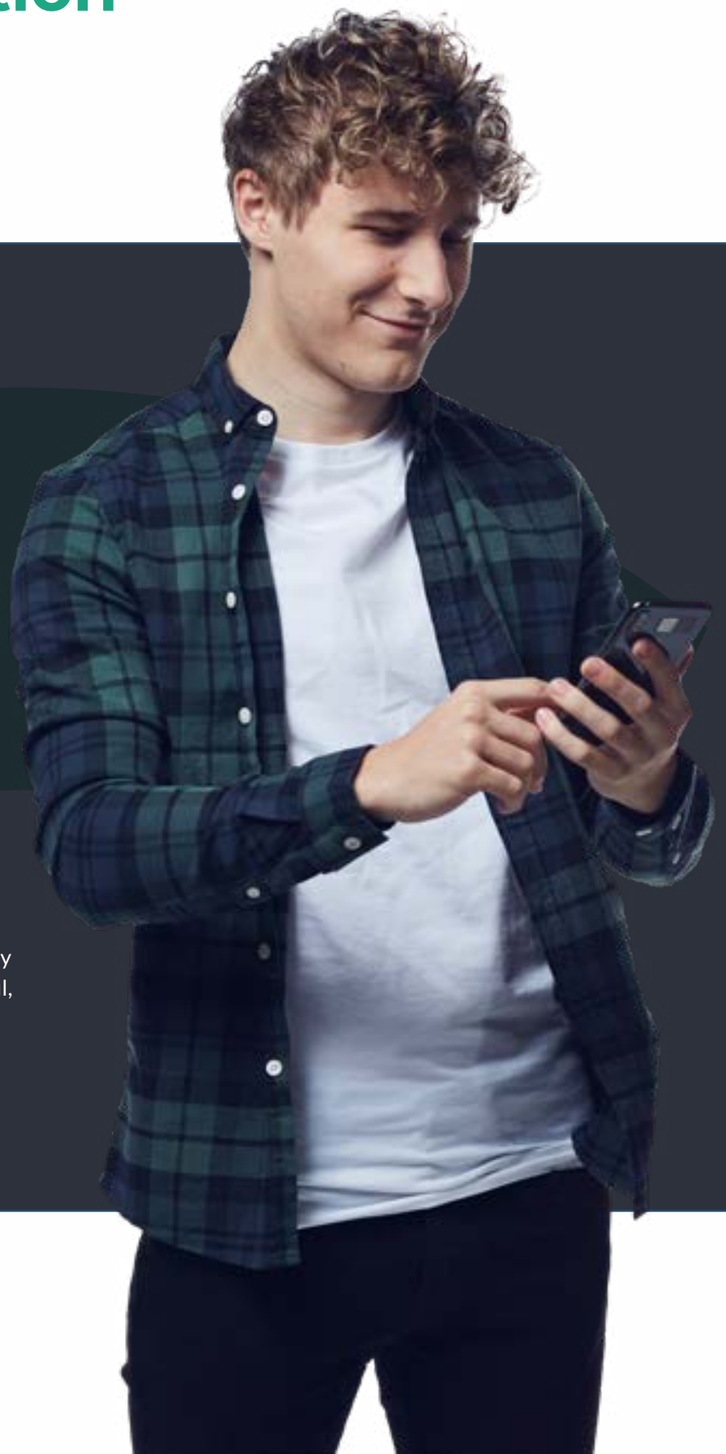
UX and security teams will need to collaborate to deliver this, investing in fraud solutions that provide the right level of passive checks and orchestration capabilities to truly put customers at the center of the transaction – no matter the channel or device they're shopping through.

[7] ***Don't Let a Slow Website Kill Your Bottom Line:*** *https://www.forbes.com/sites/rogerdooley/2012/12/04/fast-sites/#2715220e53cf*

[8] ***PWC Global Economic Crime and Fraud Survey 2018:*** *https://www.pwccn.com/en/services/consulting/forensic-services/economic-crime-survey.html*

SECTION FOUR

Callsign solution



Who is Callsign?

Callsign has a simple vision: we want to make digital identification simple and secure, every time, and across any transaction.

Our unique positive identification approach allows good users to interact online safely, with minimal friction, while ensuring that bad actors are blocked to protect customers' identities and merchants' interests at every step.

Our capabilities have been developed by individuals with a true understanding of the challenges our customers face. The core Callsign development team have worked in ecommerce, banking, and telecom organizations.

In addition to understanding the latest security tech, we also understand how to make it useful, appropriate, and practical for our customers.

An intelligent solution to complex fraud

In a threat landscape of such complexity, and with bad actors growing ever more innovative, fraud prevention must be equally intelligent. The best response for merchants is investing in fraud prevention that goes beyond spotting threats, and into positively identifying real users.

To achieve this, merchants need to embrace machine learning (ML) and Artificial Intelligence (AI) capabilities to their full potential. By analyzing an array of data across device, location, and behavior, merchants can positively identify customers in a single authentication action with results presented as an individual score.

If the confidence score is high, transactions can be safely approved. If it's not, further authentication requests can be triggered dynamically, with different levels of intervention in real time. For customers, this leads to the best possible user experience – while merchants can enjoy peace of mind and certainty that every 'good' transaction will be allowed to take place, minimizing cart abandonment and the risks of fraud.

Callsign uses a range of collection technologies, including:

Device Fingerprinting
Identifies the user through device attributes without the need for a persistent cookie on the device.

Location
Verifies that the location of the user is accurate, including if they're using a VPN.

Behavioral Biometrics
Identifies-specific attributes about a user's behavior, such as how a shopper types, swipes, or holds their phone.

Callsign's approach

Callsign detects and prevents fraud while maintaining positive experiences for genuine customers. When a user attempts to transact online, we take them on a passive multi-layered journey that adapts dynamically as required.

1

First line of defense:

Screening for bad actors

Firstly, Callsign ensures that the session is secure.

We identify and deal with threats, such as malware, bots, remote access trojans (RATs), Telco Redirection Attacks, and compromised devices. We then highlight users who are deliberately attempting to mask their identity using privacy networks or proxies.

2

Second line of defense:

Intelligence Driven Authentication

Once Callsign has established that the session is secure, we positively identify users, ensuring that they are who they claim to be.

Callsign's industry-leading AI uses advanced behavioral biometrics, location analysis, and device fingerprinting techniques to determine the user's identity. As a result, we're able to stop a bad actor gaining access to a legitimate user's account, even if they know their username and password.

3

Third line of defense:

Decisioning

If the user is genuine, they're allowed access seamlessly. If a risk is detected, they're routed to step-up authenticators.

Callsign then orchestrates the rest of the user's digital journey, passing them through whatever controls and processes your organization deems necessary. If a risk is detected during the session, Callsign will also intervene in real time to prevent the user coming to harm.

4

Fourth line of defense:

Review and refine

Finally, Callsign gives you the ability to review the effectiveness of your end-to-end user journey, and easily improve banking processes where required. Our technology makes it easy for nontechnical audiences to review the user journey and analyze data effectively, before going on to refine the journey, conduct A/B testing, and modify processes and policies.

The Callsign user journey

New customer registration

New account opening fraud – using synthetic identities or impersonation – is a serious issue for merchants, especially at a time when many are seeking to minimize friction and make opening an account as easy as possible.

Our technology protects against this, ensuring the person opening the account is who they say they are. Better yet, this information can be used to speed up further verification processes in the future, helping to provide better experiences for genuine customers.

Shopper fills basket:
The user browses an online store, selects items, and begins the checkout process.

Confirm:
The user is prompted to fill in payment details. Our threat detection filters out bad actors, while behavioral biometrics, device ID capabilities, and location data create a unique user profile.

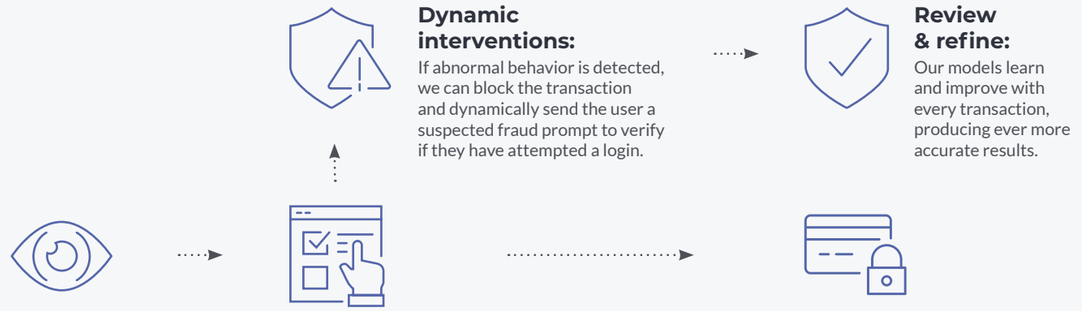
Identify:
If required, the user is routed to an appropriate identity verification provider. We'll also run telephone number verification checks to validate the data.

Order complete:
The user is prompted to create an account and password. Once a payment is accepted, payment data is stored and the account is hardened against ATO.

Return customer login

Keeping customer accounts safe from ATO, credential stuffing, and bots is crucial for maintaining security, trust, and your reputation.

When bad actors try to gain access to a genuine customer's account, our technology references thousands of points of data, including some that can't be copied by a fraudster – like the way a customer holds their phone.



Pay (screen):
As the user enters the checkout, our device ID and location intelligence identify the user and route them on a personalized journey.

Login (confirm):
Our AI and ML analyze thousands of data points across device, location, and behavior to confirm the user is who they say they are.

Dynamic interventions:
If abnormal behavior is detected, we can block the transaction and dynamically send the user a suspected fraud prompt to verify if they have attempted a login.

Review & refine:
Our models learn and improve with every transaction, producing ever more accurate results.

Fast and secure payments:
The user's details are pulled into a gateway. We optimize payment processing to limit authentication step-ups.

Guest Checkout

Not every shopper wants to set up an account to complete a purchase, but without this additional layer of verification, blocking fraudsters becomes harder.

Our technology references a huge number of data points to ensure potential fraud is blocked, and can also flag devices with suspicious activity from future use.

Screen:
As the user enters the payment process, we passively detect and block threats including malware, bots, and RATs.

Payment:
The user enters their payment details, which are processed via the gateway.

Review & refine:
If the purchase is deemed fraudulent or a chargeback is detected, merchants can pull data logs of devices to flag as suspicious in the future.

SECTION FIVE

Welcome to the world of Positive ID

A new world of connected, authenticated people

In the digital world, trust between shoppers and businesses is vital. But building trust in the digital realm is challenging, especially as customers and merchants alike grow more aware of the risks. At a time when businesses need to balance protection and experience in the way customers deserve, old methods of authentication and rules-based protection are no longer fit for purpose. We believe that authentication should be about people, not processes. Identifying bad actors should be a natural by-product of confirming that people are who they say they are. And while experiences should be seamless, privacy should always be protected, too.

That's why our approach transforms the online authentication experience from a process-driven interruption of the user experience, to a friction-free path to safe transactions and purchases. We focus on the individual, applying AI and ML to understand user patterns and intelligently adjust authentication journeys in real time, positively identifying real users while blocking bad actors.

Our dynamic authentication ensures that lower-risk transactions proceed with minimal disruption, while ensuring an appropriate level of security for more significant activities. For example, a customer may welcome more rigorous verification procedures when making an expensive acquisition than for a minor everyday purchase.

This gives merchants peace of mind in regard to online security, full compliance with regulations, and crucially, the smoothest, most transparent user experience – meaning genuine customers can get on and make purchases successfully. It offers a perfect balance between UX, fraud prevention, and compliance, reducing friction and fraud simultaneously while enabling greater collaboration between departments.

Think positive

As long as merchants sell online, fraud will always be a risk. And bad actors will always be ready to seize any opportunity. But even as fraud becomes more sophisticated and advanced, so too do fraud prevention methods powered by ML and big data.

Callsign's solutions give merchants peace of mind, the ability to meet compliance standards, and certainty in security – all while improving the user experience. Organizations that offer the easiest options for authentication without compromising security will win the long-term trust and loyalty of their customers and employees.

callsign®

Discover how AI & machine learning can help you deliver robust authentication judgements in our Machine Learning Fusion whitepaper.

Or get in touch for a demo of our capabilities: **sales@callsign.com**