THREATS SERIES

WHITEPAPER

Protecting financial organizations from fraud

How can banks keep their businesses and customers secure, while improving user experience?

OVERVIEW

Banking in a digital world

Banks are always on the front line of digital identification and fraud prevention

The products they provide, the range of customers they deal with and the sums of money they manage mean their businesses will forever be a target for malicious actors. However, evolving customer expectations and the need to improve service means that security measures can't come at the cost of experience.

Things become even more complex when you factor in regulatory pressures such as CCPA in the US, or GDPR and the move toward open banking under PSD2 in Europe. Banks are expected to be the protectors of digital identities, whist being at the forefront of innovation and service. All at a time when the number and range of threats is also growing, with UK bank transfer scams rising by 40% in a year, and 60% of banks around the world experiencing an increase in fraud volume.

The events of 2020 have now brought a new level of complexity. The gradual move to online and mobile services suddenly peaked when physical banking was temporarily taken off the table. By necessity, online-only quickly became the norm, especially via smartphone; and with it came the need to tailor user journeys by demographic. Now, more and more people are using cashless payments, online banking and mobile devices – including older consumers. Indeed, a recent Deloitte report found that only 6% of banking customers did not use an online service during the COVID-19[2] outbreak. At the same time, McKinsey research shows that between 60 to 85% of consumers prefer to make everyday transactions digitally – even those who are 65 and older.

The issue is that this confidence isn't matched by the necessary caution online. This can be particularly significant for banks, who in many countries bear regulatory responsibility for protecting their customers.

YouGov research for Callsign in 2020[3] found that people aren't increasing their security consciousness to meet their online activity. For example, over half (55%) of banking customers don't intend to update their login details, despite increased fraud risk. Instead, most are content to leave things as they are, with only 19% having updated their banking login details in the last month. If customers aren't taking security precautions, banks are the final – and sometimes the only – line of defense against fraud.

However, it's also important to consider the impact of customer experience on banking and fraud prevention. Across the digital world, customers are enjoying friction-free, efficient and personalized services. Understandably, they also want that from banks, and with customers increasingly driven by convenience over loyalty, there is a clear business case for service-focused innovation. But sacrificing security opens up the door to fraud vulnerabilities, particularly when banks lean on traditional rules-based authentication that struggles to keep up with the fast-paced digital world.

Combined, these issues mean that banks' fraud prevention strategies and technologies must be first-rate.

Squaring customer demands with anti-fraud measures

A large part of the challenge banks face around fraud and customer experience is rooted in change within their own businesses. Fraud prevention was once a job for dedicated security departments. Now, with service an increasing priority in banking, fraud prevention involves multiple teams spanning customer experience, innovation, data, risk and compliance, each of whom have their own specific objectives. By their nature, omnichannel user journeys cross multiple devices and touchpoints – in the process, becoming more complex and harder to follow. Meanwhile, disparate systems can separate customer data into silos, creating weak points and increasing costs by replicating work and technology.

There are also budget considerations, with anti-fraud solutions often becoming expensive when purchased for an isolated need. Even if banks budget for the initial investment, it's the long-term costs that come as a result of increased fraud and diminished customer experience that aren't always accounted for.

Ultimately, this means that banks need robust, effective and intelligent new ways to tackle the persistent challenge of fraud. And they simultaneously need to avoid the friction that harms experiences and discourages customers.

[1] *Number of bank transfer scams in UK rises by 40% in a year:* https://www.theguardian.com/money/2019/sep/26/number-of-bank-transfer-scams-in-uk-rise-by-40-in-a-year

[2] *COVID-19 boosts digitalisation of retail banking:* https://www2.deloitte.com/ch/en/pages/financial-services/articles/corona-krise-digitalisierungsschub-im-retailbanking.html

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

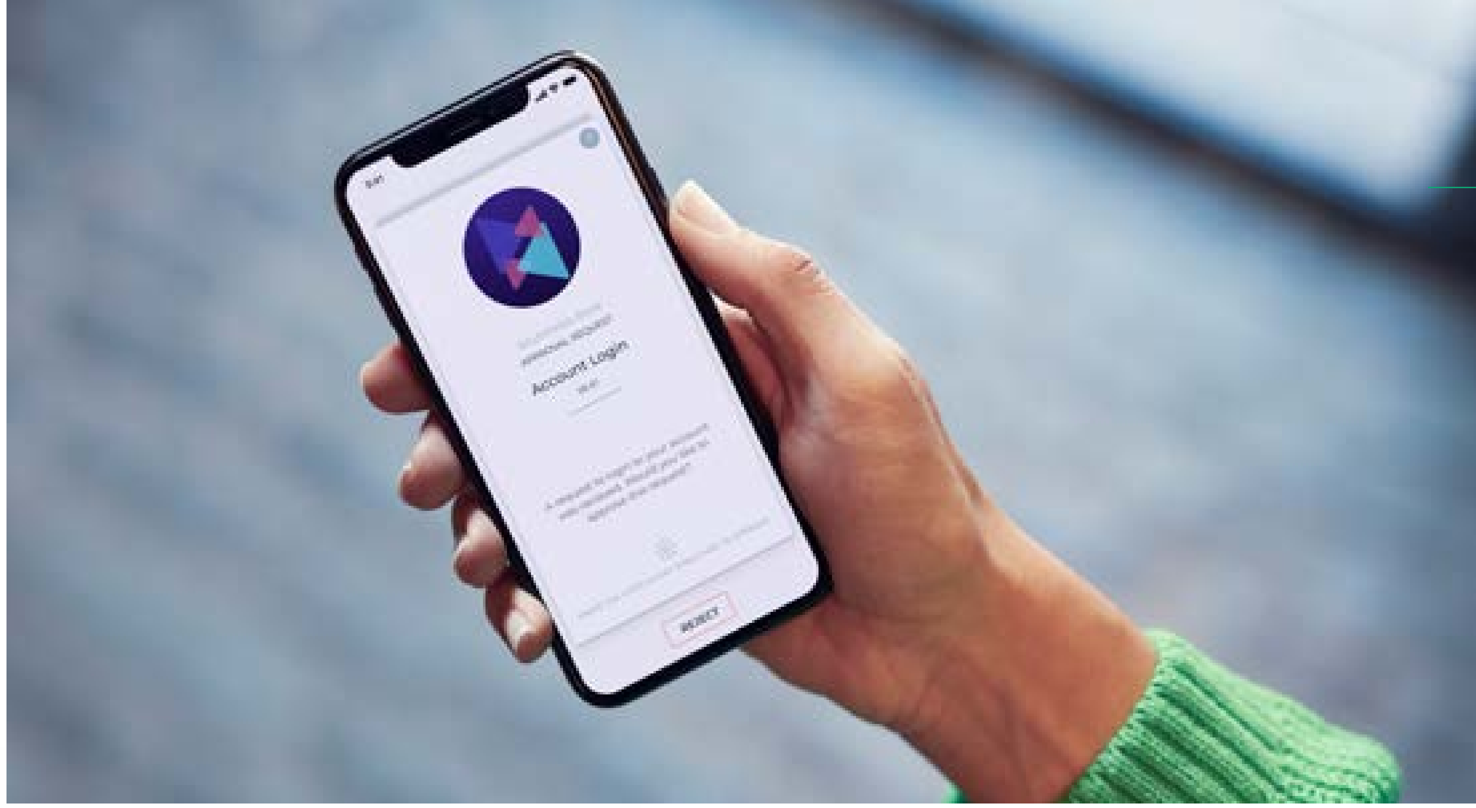
SECTION TWO

The scale of the challenge: What banks are up against

The fraud challenge banks are facing is more complex and nuanced than ever

Fraud is getting harder to detect. The vectors under attack are evolving as bad-actors get more innovative, and often the measures banks have to take to avoid fraud add friction into the customer journey.

Overcoming this requires focus. A recent banking fraud survey by KPMG[4] found that 61% of respondents said the total volume of external fraud had increased. And while increasingly sophisticated attacks are hard to combat, there are some key security issues for banks and financial institutions that can be looked at now. Understanding the different ways that bad actors operate is the first step to finding the solution banks need to thrive securely in the coming years.



Social engineering

A fraud vector that has been on the rise for years now, social engineering involves bad actors impersonating a bank or credit card provider (or other organization) to manipulate victims into revealing personal or financial data. This is often made more believable with small amounts of real data obtained elsewhere.

The most common social engineering attempts are by phone or email, asking for a password, PIN or other confidential information. The attackers may pretend to be a call center agent or similar to gain access. Naturally, the areas of access for social engineering fraud have grown with the amount people share on social media, and a report by Accenture[5] found social engineering to be the second most costly form of attack for banks.

It may include:

APP (authorized push payment): As real-time, irrevocable money transfers become more popular, bad actors have started deceiving victims with requests for payment directed to the bad actor's bank account. This generally takes the form of a bad actor hacking a customer's email and pretending to be a representative from a service or business they use (such as a solicitor or builder). They will claim to have a new account and request payment to it.

Alternatively, the scammer may claim to be the customer's bank, informing them they have been the victim of fraud and suggesting that they move their money immediately. In both instances, the customer may act and make payment before realizing – too late – that they have been defrauded.

This can involve significant sums. For example, in property payment fraud, bad actors may intercept the email chain between sellers, buyers, realtors and attorneys to divert a large payment. They are also prevalent in B2B banking, with scammers posing as genuine suppliers or the bank asking for money. In these cases great care is paid to replicate the look and feel of the bank or supplier, targeting businesses who have used the legitimate payee in the recent past, and requesting money via a real-time scheme.

Man-in-the-middle: One of the oldest types of cyberattack. Criminals intercept information between two parties who think they are communicating directly, either by interfering with legitimate networks, or creating fake networks to strip comms of any encryption. This allows the attacker to steal login credentials or personal information, spy on the victim, sabotage communications, or corrupt data.

[4] *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

[5] *2017 Cost of Cyber Crime Study:* https://www.accenture.com/gb-en/insight-cost-of-cybercrime-2017

Account opening fraud

As organizations try to offer the most seamless experiences possible, they may reduce authentication and verification requirements, leaving their platforms open to account opening fraud (also known as new account fraud or online account origination fraud). Here bad actors use stolen or synthetic identities to open new bank accounts, usually maxing out credit limits within 90 days. This can include ordering authentic physical cards to get cash. Account opening fraud is emerging as one of the biggest concerns for retail banks due to the rise in demand for cashless payments and online banking. As such, it should always be a consideration. The use of real details means that fraudulent applications may not be detected until weeks after the account is opened.

Attempts may include:

Synthetic IDs: These are identities created by combining personal details of more than one person. A report from the Aite Group[6] in 2019 found that 65% of fraud experts believe that synthetic identities are a bigger issue for banks than regular identity theft.

Multiple applications: Bad actors may create seemingly legitimate firms, which open several accounts with different synthetic identities at once. They can then work to build each account's credit score by creating interactions between the different fraudulent IDs.

Impersonation: This may incorporate genuine but falsely obtained documents, such as passports or National Insurance cards, or counterfeit documents. Information might also be obtained from correspondence, such as bank statements or bills, or through open sources such as social networking sites and births and deaths registers. Data can also be accessed from social engineering scams.

Account takeover (ATO)

Many account takeovers originate from data breaches (although they may also stem from phishing emails or social engineering). These instances often see data from large breaches refined and sold on the dark web, either by individual dataset or in aggregate. But in any approach, criminals get the data they need to mimic a user's identity and infiltrate customer accounts to take control.

ATO can include:

Credential stuffing: In manual or automated account takeover attempts, bad 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. Bots are often at play for much of the work here, including data mining and validating stolen credentials. They can be used for both credential stuffing and brute force attacks.

Telecoms fraud

Criminals are well aware of telecommunication providers' reliance on two-factor authentication (2FA) transactions. As a result, they continue to exploit these methods, weakening and abusing systems for their own advantage. Fraudsters commonly practice SIM-swap fraud – whereby they obtain personal information about the victim to then contact the target's mobile operator, claiming that their phone has been lost or stolen.

With a decline in customers visiting stores in person, operators become reliant on channels that are more open to manipulation to service their customers.

[6] *Aite Group: Current and Future FI Fraud Loss Trends:* https://aitegroup.com/report/current-and-future-fi-fraud-loss-trends-it%E2%80%99s-time-new-technology-investments

A number transfer is authorized after the fraudster has gained the confidence of the mobile operator, and the number is activated on a new SIM card. In doing so, the fraudster is granted access to the victim's number and is able to retrieve all one-time passwords (OTPs) and authentication codes sent to it. This is a growing problem. In March 2020, Europol revealed that SIM-swap scams were on the rise across Europe, after an investigation had led to the arrest of 12 suspects associated with the theft of more than €3 million ($3.3 million)[7].

However, it's important to note that SIM-swap fraud is not the only option fraudsters have to intercept OTPs from their victims during COVID-19 and in the long-term. It also includes:

Call divert: Bad actors mine user information from other sources and use it to ask the network provider to set up a call divert, forwarding or redirecting incoming calls to an alternate number. As a result, all calls to the legitimate phone number are routed to the bad actor, creating the same issues as a SIM swap.

Social engineering: In addition to the growing numbers of SIM-swap attacks, malware and remote access applications on mobile devices provide further streams for fraudsters to steal SMS OTPs. For instance, individuals are socially engineered to download remote access apps, such as TeamViewer or hidden surveillance apps. These either give fraudsters remote access to the victim's device, allowing them to directly read their messages, or silently record all their texts and phone calls to forward to another device. Here, the victim's private messages – including OTPs – are intercepted by the fraudster in the same way a SIM-swap attack does. However, in this instance the victim is unaware as the fraudster has direct access to their device.

Multi-party challenges: Finally, several parties are involved in the delivery of OTPs, so each provides a chance for messages to be captured. As such the potential for mass compromise becomes quite large, particularly when taking into consideration the underlying vulnerabilities and attack surface of Signaling System No. 7 (SS7), a set of protocols which allows phone networks to exchange the information required for calls and text messages. Banks need to adopt a clear view of all data sub-processors and make sure they each have suitable security controls in place, for example multi-factor authentication (MFA), audit logs, and dashboards. Similarly, all telephone numbers need to be auto-redacted to minimize the impact of data breaches.

[7] https://www.europol.europa.eu/newsroom/news/sim-highjackers-how-criminals-are-stealing-millions-highjacking-phone-numbers

SECTION THREE

Balancing security with customer experience

With so many different types of fraud on the table, there's no doubt that security is vital to banks and other financial services firms

But if security protocols disrupt customer journeys or hinder employees while working, the friction produced can cause real problems – including a loss of customers and reputational damage.

These problems can arise from varying levels of accessibility for many popular authentication methods. SMS OTPs may not work in areas with poor signal; fingerprints may require privacy acceptance; and facial recognition might be complicated by everything from sunglasses to masks.

And for long-established industry players, these issues have been further exacerbated by the growth of digital-first innovators who prioritize modern approaches to service delivery.

The perpetual issue is that cracking down on security can create an exasperating user experience. Keeping out the 'bad' transactions can come at the cost of a smooth experience for the 'good' ones, and an approach to security that produces a lot of false positives can be more costly than the fraud you're trying to prevent. Sadly, this is a common issue. In a PwC survey,[8] 34% of respondents thought their organization's use of technology to combat fraud was producing too many false positives.

The answer for banks is finding the right balance between experience and security across every transaction. As customers expect more control over their personal data than ever before, this balance should be top priority. A solution that only adds friction where necessary – and attempts to positively identify users by using passive analysis and authentication methods across device, location and behavior – offers the best of both worlds.

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

SECTION FOUR

An intelligent solution to combat fraud

Banking increasingly demands robust security and exceptional service

Meanwhile, bad actors are growing ever more intelligent and innovative. This means that fraud prevention must be equally intelligent if banks are going to meet the demands of their customers, the need for high security standards, and stay on the right side of regulatory lines.

Embracing data and unlocking machine learning (ML) capabilities is the answer. By analyzing an array of data across device, location and behavior, financial institutions can positively identify customers in a single authentication action that meets a single possession, knowledge and inherence attribute.

With Callsign these modalities can be presented as individual scores or as one combined risk score – helping teams make more informed decisions. 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, all in real-time.

These technologies mean banks can open the door to highly efficient fraud prevention solutions that avoid disrupting the customer experience. And they are being recognized by regulatory bodies, including the European Banking Authority[1].

By using them, banks can build trust with customers who are reassured that they are managing their money securely. And this boosts affinity, as people enjoy their experiences of digital banking services, rather than enduring them.

In today's world, positively identifying a user means more than stopping a bad actor. By prioritizing correct, positive identification, based on digital DNA, banks are able to engage customers in ways they will appreciate, while reducing costly service calls and cutting the amount of fraud they and their customers are subjected to.

[1] *The 4 Key Points You Should Know From UK Finance's SCA Update:* https://blog.callsign.com/the-4-key-points-you-should-know-from-uk-finances-sca-update

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 balances high security and user experience, allowing customers to interact online safely, with minimal friction, while ensuring that bad actors are blocked to protect customers' identities and merchant's 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 come from banking, eCommerce, and telecom organizations. In addition to understanding the latest security tech, we also understand how to make it useful, appropriate and practical for our banking customers.

Callsign offers complete Strong Customer Authentication capabilities across:

Possession:
We identify the user through device fingerprinting attributes without the need for a persistent cookie on the device.

Inherence:
We identify specific attributes about a user's behavior, such as how they hold their phone, how they swipe or how they type.

Knowledge:
Whilst we can offer traditional knowledge-based authenticators such as PIN and password, we always recommend layering these with inherence-based attributes such as keystroke dynamics to ensure they offer the appropriate level of protection.

Callsign's approach

Callsign detects and prevents fraud while maintaining positive experiences for genuine banking customers. When a user begins an online interaction, from account opening to making a payment, we take them on a multi-layered journey which 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 are 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 are allowed access seamlessly. If a risk is detected, they are 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

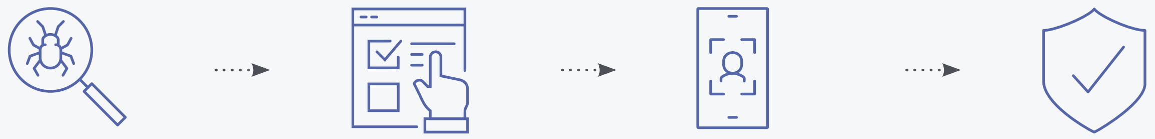
Finally, Callsign gives you the ability to review the effectiveness of your end-to-end user journey, and easily improve banking processes where required. Our technology makes it easy for nontechnical audiences to review the user journey and analyze data effectively, before going on to refine the journey,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

The Callsign user journey

Opening a new account

New account fraud is ever present in banking, with fraudsters seeing it as an ideal entry point, and where tactics like synthetic identity and impersonation can grant access to customer accounts.

Our technology helps banks by using contextual data combined with third party data, such as SIM swap detection, to confirm the user is who they say they are. This information can also be saved for the future, to speed up processes and improve the customer experience.



Screen:
User navigates to application form, in the background Callsign passively detects and blocks threats including malware, bots and RATs.

Confirm:
User completes the application and Callsign runs checks to confirm their identity.

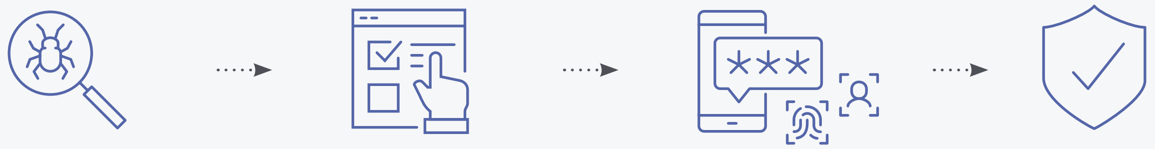
Identify:
User is routed to identity verification and affordability checks, such as credit checks.

Review & refine:
Audit trail established and user profile created to be used to prevent future account takeover attacks.

Logging in

The login stage is often where bad actors gain account access through social engineering, credential stuffing bots, or account takeover. For banks, this is where experience meets security in the most nuanced way.

Blocking fraudsters is essential at login. Our technology gives banks the tools to do that by referencing data points that bad actors can't emulate, such as the way the genuine customer holds their phone or types. So banks are far more able to keep fraudsters out, while providing legitimate users with a smooth login experience.



Screen:
The user logs in, and Callsign passively detects and blocks threats.

Confirm:
Callsign's AI and ML models analyze thousands of data points across device, location and behavior to confirm the user is who they claim to be.

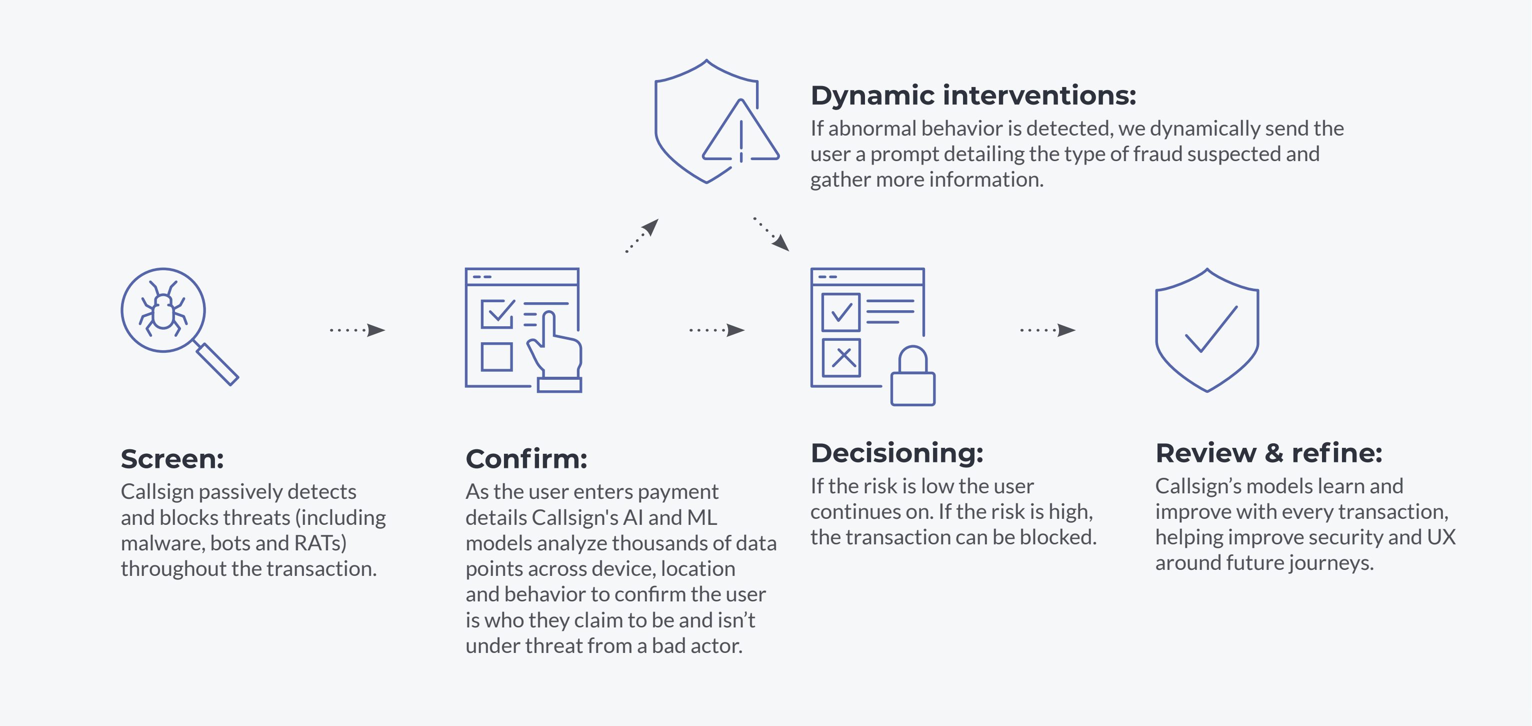
Respond:
If the user cannot be positively identified they are routed to step-up authenticators.

Orchestrate the journey:
Callsign positively identifies legitimate users, reducing friction throughout their session.

Making a payment

Payments and transfers open up a host of potential fraud attack vectors. Fraudsters are liable to try social engineering, account takeover, APP fraud, credential stuffing and bots to trick customers out of their money.

Our solution again references data points that bad actors can't replicate, recognizing abnormal behavior in real time, and dynamically intervening if necessary. This reduces the burden on your customers, while helping to counter some of the most complex methods of fraud there are.



Dynamic interventions:
If abnormal behavior is detected, we dynamically send the user a prompt detailing the type of fraud suspected and gather more information.

Screen:
Callsign passively detects and blocks threats (including malware, bots and RATs) throughout the transaction.

Confirm:
As the user enters payment details Callsign's AI and ML models analyze thousands of data points across device, location and behavior to confirm the user is who they claim to be and isn't under threat from a bad actor.

Decisioning:
If the risk is low the user continues on. If the risk is high, the transaction can be blocked.

Review & refine:
Callsign's models learn and improve with every transaction, helping improve security and UX around future journeys.

SECTION FIVE

Welcome to the world of Positive ID

A new world of connected, authenticated people

Banking relies on trust and reassurance between financial institutions and customers. Without that, people lose faith in banking, and banks lose business to competitors who understand and prioritize it.

We believe that trust in finance is about protection as well as experiences. Reducing the risk of fraud, while providing customers with constantly evolving and improving services. For online banking, this is still a work in progress, with banks having to earn the trust of customers and retain it as they have in the offline world.

That's why our approach is to positively identify the customer, which 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 apply AI and ML to understand user patterns and intelligently adjust authentication journeys in real time. This dynamic authentication brings together UX, fraud and compliance in a holistic solution that reduces friction, eliminates fraud, and encourages greater collaboration between departments. Positive ID ensures that lower-risk transactions proceed with minimal disruption, while ensuring an appropriate level of security for more significant activities.

This gives banks 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 work with banks successfully.

SECTION SIX

Think positive

Digital services are here to stay for banks, so fraud will always be a risk. And bad actors will always be ready to seize any opportunity. At the same time, customer expectations and demands are evolving, asking more of banks who need to see any security changes they make through the lens of service.

This makes fraud prevention methods powered by ML and big data essential for any bank wishing to modernize its services, improve fraud detection and prevention and maintain customer trust.

Unfortunately, traditional authentication and rules-based protection is more harmful than helpful for modern banking. Today, banks need to create personalized journeys and balance protection and experience. In the age of putting the customer first, many forms of fraud protection put the individual last. The right approach for banking should start with the individual, using the characteristics that make each of us unique to make digital life smoother and safer for customers.

Callsign's solutions do just this, giving banks peace of mind, the ability to meet compliance standards, and certainty in security – all while improving the user experience. Organizations that offer a degree of choice during authentication will be the ones to win the long-term trust and loyalty of their customers and employees.

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**