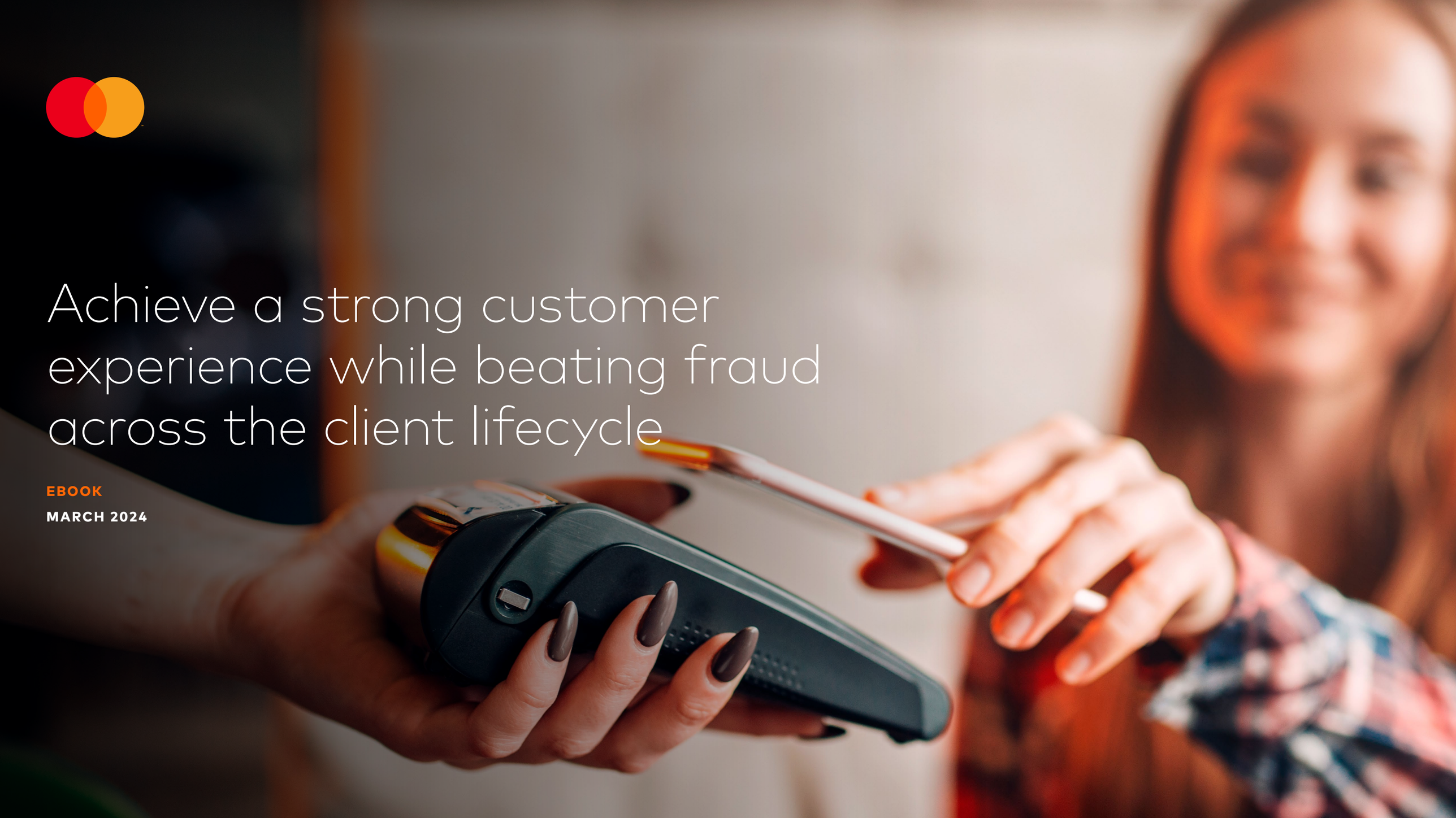


Achieve a strong customer experience while beating fraud across the client lifecycle

EBOOK

MARCH 2024

Contents

Achieve a strong customer experience while beating fraud across the client lifecycle

This white paper underscores the dual imperative for financial institutions (FIs) to enhance the customer experience and fortify fraud prevention across the client lifecycle. Emphasising the significance of client lifecycle management (CLM), the paper navigates challenges posed by evolving consumer expectations, sophisticated and evolving fraud tactics and organisational siloes. A solution framework is suggested, advocating for better data utilisation and dynamic workflows. Furthermore, the paper introduces the importance of behavioural data insights that can optimise the identity verification process, improve risk decisioning, enhance customer experience and reduce associated costs.

In essence, the white paper advocates a proactive, holistic CLM strategy aligning with market trends, regulatory demands and technological advancements. By leveraging advanced machine learning (ML) tools and breaking down organisational siloes and barriers, FIs can simultaneously elevate customer experiences and fortify defenses against evolving fraud threats throughout the client lifecycle.

Consumers in today's digital world expect speed and ease in every online interaction, including with FIs. This means providing a safe and low-friction experience throughout the entire client lifecycle—from onboarding to log-in to transactions—is essential to building, growing and keeping your book of business.

A quick definition: Client lifecycle management

While the client lifecycle comprises the journey your clients take to becoming a customer and subsequently interacting with your company, **CLM** is the holistic approach to managing that relationship. This includes everything from the first interaction with a potential client through onboarding and retaining these customers and eventual offboarding. Regulatory compliance is an essential piece of this work—including KYC/AML checks—along with the processes, both manual and automatic, that enable a smooth, compliant experience.

Ultimately, an effective CLM strategy for financial institutions means protecting both your business and clients from the moment they begin an online application through every subsequent interaction. This must be done while providing the best experience possible—all with the intent to keep clients with your company for as long as possible.

Market landscape

When looking at the current market landscape that FIs are operating in—and therefore, what's driving the need for CLM innovation—there are several key influences, such as:

Accelerated digital growth that shifts consumer expectations around speed and ease

Lengthy account opening processes that can delay revenue realisation

Competition that makes it easier for consumers to leave after one bad experience

Enhanced scope of regulations and associated costs

Digital growth and customer expectations

Customers now expect to be able to do business anywhere, anytime. Depending on country requirements, customers may accept more friction. For example, because Germany has regulations that require a face-to-face conversation (in person or online) to open a new account, consumer know to expect this step of the onboarding process. Still, all customers expect a seamless experience during moments like log-in and account modification.

This means FIs are tasked with rebalancing their CLM strategy to focus more on satisfying customers throughout the lifecycle while still adhering to regulations and performing the risk checks that keep the business safe. Because, ultimately, fraud isn't always captured during regulated checks at onboarding. In fact, according to Datos, synthetic identity incubation—which often slips under the radar during KYC/AML checks—was one of the top three (tied at number two) most common types of fraudulent activity observed from demand deposit/checking account applications in 2022.

Global regulations

Local laws, regulations and policies that govern the financial industry change on a near-constant basis. This means that maintaining compliance throughout the entire client lifecycle can be particularly challenging. The repercussions for not maintaining compliance can be severe—both in terms of monetary penalties and lost trust from clients. That's why FIs benefit from viewing compliance as a key piece of CLM—from onboarding and KYC/AML through transactions.

To illustrate its importance, banks and other financial institutions across the globe were fined almost $5 billion for AML infractions, sanction breaches and KYC shortcomings in 2022. It's clear that prioritising compliance throughout the client lifecycle is as important as ever.

Furthermore, there is a **growing focus on artificial intelligence (AI) and machine learning (ML)** within the financial services industry. These powerful technologies foster innovation when stopping fraud while also promoting financial inclusion.

Meanwhile, new regulations continue to be passed and enforced across the globe, including the UK's Economic Crime and Corporate Transparency Bill 2023 and Canada's Forced Labour and Child Labour in Supply Chains Act 2023, both of which are aimed at fighting financial crime across multiple jurisdictions. It's essential to find a way to build scalable processes for maintaining regulatory compliance while balancing those needs with customer experience.

In 2022,
financial institutions were fined

$5 billion

for AML infractions, sanction breaches and KYC shortcomings.

Key challenges

With those driving forces in mind, what are the challenges FIs face when attempting to transform their CLM strategy? When looking at the problem holistically—that is, from account opening through management and transaction—there are three key buckets these challenges can be broken into:

1

Changing customer expectations in the digital age

2

Shifting and sophisticated fraud tactics

3

Siloed and legacy technology

Changing customer expectations

Changing customer expectations in the digital age are as much a driver of shifting CLM needs as they are a challenge. Finding ways to decrease unnecessary friction in the customer journey while still meeting regulatory requirements is an increasingly difficult line to walk.

In this **survey,** we asked more than 7,000 consumers across North America and Europe what they wanted in their digital account experiences. Almost 65% reported abandoning their account opening or transaction process on at least one occasion due to friction, including the process taking too long.

For FIs to meet rising customer expectations, fraud prevention that doesn't impede any stage of the client lifecycle is essential. Ultimately, this means finding ways to increase automation, enabling FIs to gather the same amount of information and insights while decreasing the burden placed on consumers.

From speed to security consumers are demanding more from their digital experiences with companies...

73%

agree that when they are trying to create an account or process a transaction on a modern digital platform, the process should happen instantaneously

75%

admit that they do not have patience for sub-par digital experiances due to the choice available to them

77%

consider security, trust and data privacy to be more importnant than convenience, speed and ease-of-use when creation an account or making a transaction using a company's digital platform

Shifting and sophisticated fraud tactics

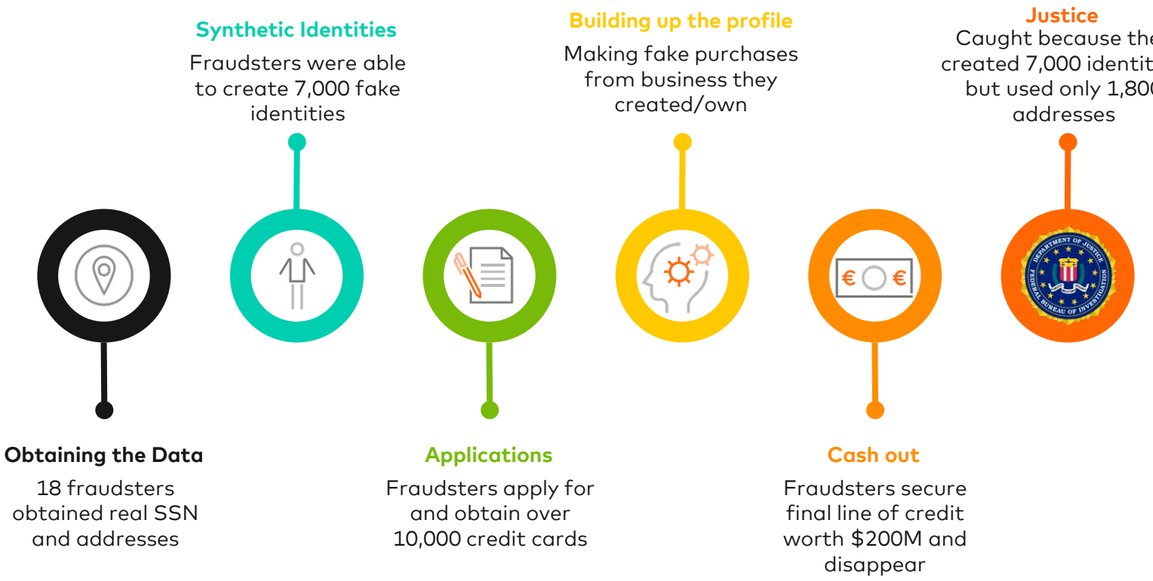
With the proliferation of AI technologies, a "democratisation of fraud" is underway. This means that people who might otherwise not have had the ability to perpetrate fraud at scale now have access to tools that allow them to cause greater damage. It is vital that FIs prepare for a new type of fraudster at their doors.

New account fraud that's conducted using long-standing **synthetic identities**, created by merging genuine information with fabricated information to create a new "identity," continues to be a large pain point for FIs. The real identity data involved—gained easily by purchasing PII data on the dark web as a result of data breaches enables fraudsters to slip under the radar of identity verification checks that only validate traditional, primary data elements and are only tangentially related to digital identity.

For example, while phone number, email address and postal address are the most used identity elements to create synthetic identities, KYC checks don't look at the relationship between these elements. This means that even with strict regulatory requirements imposed during onboarding, synthetic identity fraud is projected to cost businesses nearly **$5 billion** in 2024.

Account takeover fraud is also on the rise. Fraudsters' tactics involve exploiting weaknesses in web applications to steal personal data needed to access an account. In other instances, they might launch malicious bot attacks to steal data. It's predicted that the cost of global cybercrime data breaches across all industries will grow to more than **$5 trillion by 2024**. This means determining when and how to perform the right risk checks to identify fraudulent activity without impeding on the customer experience is key.

"Eighteen people charged in international $200 million credit fraud scam"



Source: https://archives.fbi.gov/archives/newark/press-releases/2013/eighteen-people-charged-in-international-200-million-credit-card-fraud-scam

According to a **recent survey** of UK banking customers, more than one in four consumers are worried about ATO.

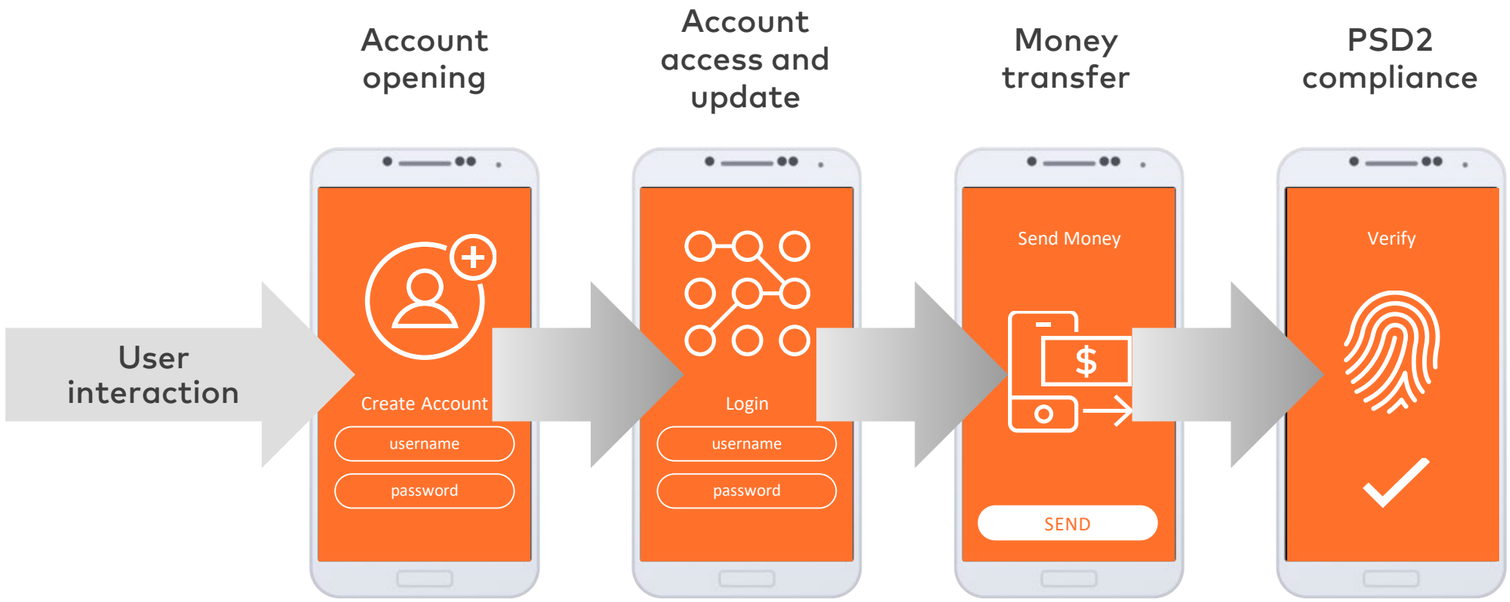
Organisational siloes

FIs often run into issues with siloes, both in terms of data and organisational priorities and functions. In fact, only **30% of banks** that have undergone a digital transformation report successfully implementing their digital strategy. This indicates that organisational siloes are often a contributing factor.

With many FIs operating in traditional functional or business siloes, there can be misaligned priorities, lacking clarity and issues in execution. This is especially relevant when implementing holistic CLM, which requires clear communication across functions and a prioritisation of customer experience regardless of the stage they're in. This fragmentation can result in different technology, data storage and more impeding a company's ability to improve customer experience while identifying fraud as quickly as possible.

How to solve for it: Better data and fewer siloes

Given the historic view of fraud prevention as a cost center, it's often relegated to a reactive, siloed role. With expanding regulations—such as the **upcoming requirement** for UK financial institutions to reimburse victims of scam fraud—combined with increased digital fraud activity, it's imperative to shift toward a more active, holistic role. This role must prioritise customer experience to ensure data is shared and, importantly, work with others to improve an FI's bottom line through a stronger CLM strategy.



- Credit card application
- New checking account
- Loan application
- Mortgage application

- Login
- Password update
- Profile update
- Reset password

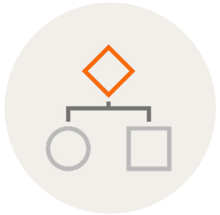
- Online payment
- Money transfer
- Add payee
- Wire send

- European payments
- Recurrent payments
- SCA-exempt transactions

Better data

It's clear that FIs don't suffer for a lack of data anymore—there is almost too much of it floating around. The hurdle comes from determining how to derive insights and then action on them appropriately—often with the assistance of machine-learning models that don't rely on static data. For example, how can an FI go beyond verifying an email address or phone number to determine its risk during onboarding or account modification?

Ultimately, FIs need to be capable of confidently verifying most, if not all, of a customer's identity—and to do it with as little human intervention (whether on the consumer or business side) as possible. In other words, achieving maximum confidence with minimal friction.



Dynamic workflows

By integrating more automated, passive touchpoints for risk assessment and identity verification before applicants get to the KYC/AML step of the onboarding process, organisations can create more customised onboarding workflows.

This means friction remains low for good customers, who are deemed low risk and hence not subject to needless step-ups, while throwing up barriers and hurdles for high-risk applicants that might be employing synthetic identities.

Relational and behavioural attributes

Mastercard has taken insights from this tracing activity, overlaying them with specific analysis factors, including account names, payment values, payer and payee history and the payee's links to accounts associated with scams. This is an example of how AI can provide banks with the intelligence necessary to intervene in real time and stop a payment before funds are lost.

Artificial Intelligence

An important piece of this puzzle is the use of AI. Mastercard is taking the fight to fraudsters with its one-of-a-kind AI powered Consumer Fraud Risk solution. Over the past five years, Mastercard has worked with U.K. banks to follow the flow of funds through mule accounts and then close them down.

Based on insights from this tracing activity and overlaying them with specific analysis factors such as account names, payment values, payer and payee history, and the payee's links to accounts associated with scams, this is an example of how AI can provide banks with the intelligence necessary to intervene in real time and stop a payment before funds are lost.

HOW TO SOLVE FOR IT: BETTER DATA AND FEWER SILOES

Overall, FIs must discover what data is necessary to secure the risk insights needed to make informed, automated decisions that enable them to further customize the user journey–all while meeting regulatory requirements. This can include building advanced ML models or distinct rule sets that are monitored and analysed regularly, ensuring fraud is caught quickly but not at the expense of good customers.

Fewer siloes

But what use is better data and insights if they aren't employed throughout the entire client lifecycle? It's important to consider how to build bridges between account opening and log-in, money transfer and account modification—as much as between fraud and customer experience.

Same technology stack

As a first step, ensure the teams who own different parts of the client lifecycle are on the same technology stack as much as possible. This helps ensure data is being captured in the same way and thus able to be ingested at all stages of the lifecycle, cutting down on how often a customer is asked for the same information, without decreasing the efficacy of risk decisioning.

Connecting data and insights

By connecting data and insights across disparate systems wherever they reside—and implementing ML-based tools wherever possible—FIs can improve security and KYC/AML compliance while also making for a smoother customer experience. For example, if a risk score is generated and captured during onboarding, that score can be ingested again upon first deposit or withdrawal to help bolster risk decisioning and determine the flow the customer is sent down.

More tangibly, capturing the identity data a customer provides during onboarding and ensuring it's available throughout the entire lifecycle means there are more insights on hand to stop account takeover before it happens without adding undue friction. This is why it's crucial to work with vendors that avoid "black box" scoring and provide you with as much flexibility as possible in their returned insights, scores and attributes.

The key is ensuring communication in the same language across the entire client lifecycle. By doing so, an FI's CLM strategy can begin to grasp a customer's risk profile more holistically, reducing friction while also ensuring regulatory requirements are met and fraud is mitigated.

How we help

With Mastercard Identity data and insights, FIs can enhance CLM, optimising the verification process and associated costs by determining the risk level of each applicant at the very first touchpoint and all the ones that come after. In real-time, fraud managers can:

- Leverage predictive, probabilistic identity data and insights provided through sophisticated machine-learning models to complement existing KYC and AML checks
- Detect bots and automated acts by using device and behavioural signals across account touchpoints
- Defend against account takeover fraud with deep device insights and behavioural biometrics
- Employ AI to help identify real-time payment scams before funds leave a victim's account

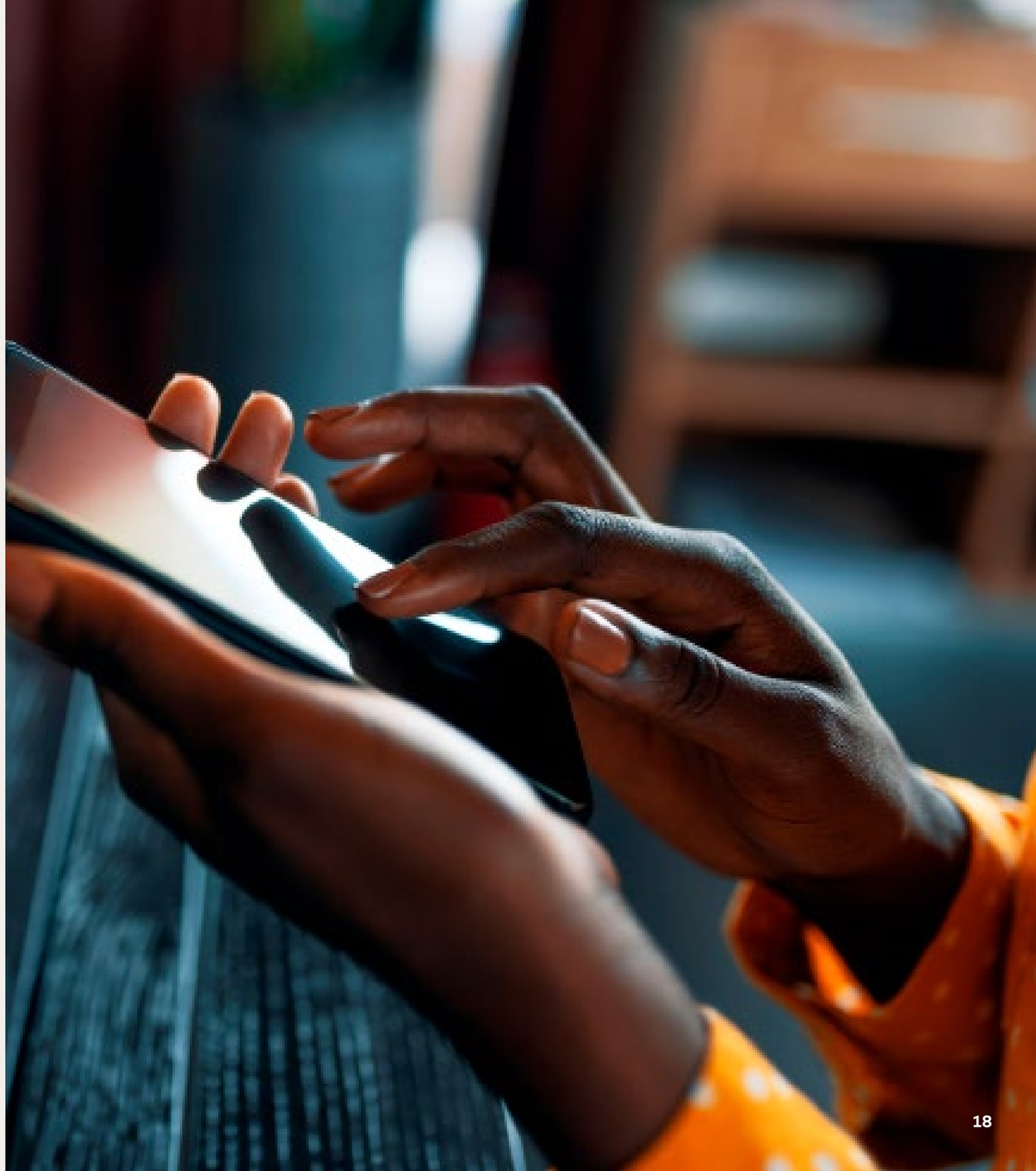
With Mastercard Identity data and insights, FIs can see the complete digital identity footprint. This includes behaviour as well as other data points—including device usage—to validate legitimate applications and interactions, such as changing a profile's email address or phone number. This not only helps stop scripted attacks at account opening, but it also increases confidence in customers and lowers friction.

The Identity Engine

The Identity Engine uses two discrete datasets to power these insights. The first, the Identity Graph, includes data gathered from more than 100 authoritative data sources and contains more than seven billion identity elements. We are continually expanding the dataset's data sources, elements and unique identities to achieve ever-greater identity insights.

The second data set, the Identity Network, includes first-party data gathered by millions of anonymous customer digital transactions each month. This amount of data, which includes international data from 238 countries and territories, is unmatched by other probabilistic assessment solutions and it only continues to grow.

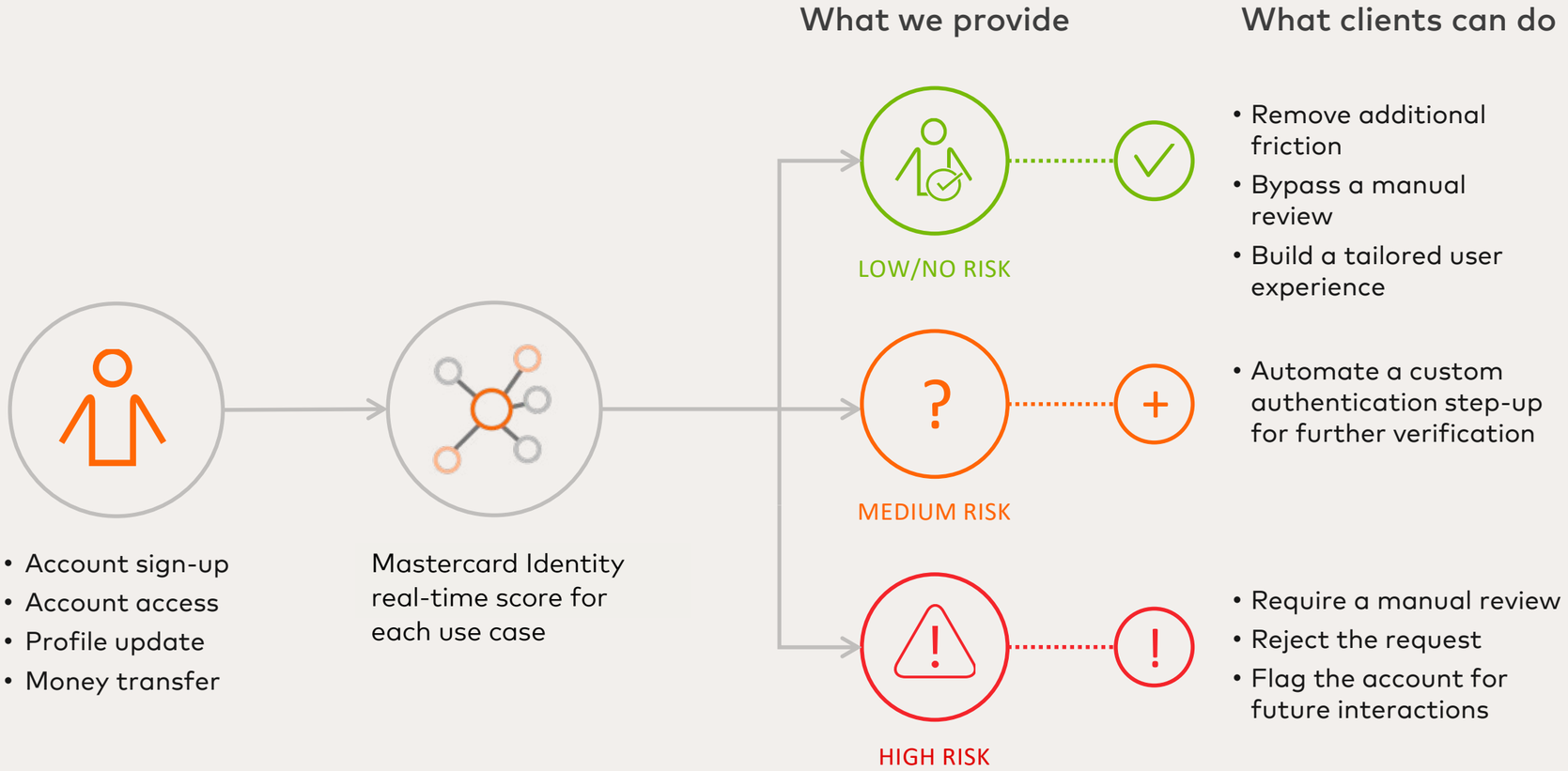
The Identity Engine applies sophisticated data science and machine learning behind the scenes to generate a probabilistic determination of the validity of the identity information. The methodology analyses linkages and activity patterns, such as how long identity elements have been in use and how they have been used in combination. The analysis derives signals that indicate the level of risk attributed to the validity of the identity information.



Real-time insights

In leveraging real-time identity and device insights, FIs can reduce the costs associated with manual review and compliance checks while increasing customer satisfaction. Importantly, these insights can be ingested at any stage of the client lifecycle, which means information gleaned at account opening can be used to further automate risk assessments performed when profile identity information is changed.

Consumers have more choices than ever before when it comes to financial services. When it comes to mitigating fraud in this ever-competitive landscape, FIs need to consider the needs of the consumer as well as their bottom line.



CASE STUDY

How Sun Finance improved risk decisioning and customer experience

Sun Finance are a rapidly growing online and mobile lending platform providing modern financial services to clients who prefer speed and accessibility and serve those historically underbanked by traditional lenders. Sun Finance operates in seven countries across three continents.

A lack of access to traditional identity data sources can mean months of trial and error as they expand into new markets. This can result in higher fraud but also more applicant drop-off, as Sun Finance finetune their decisioning model, sending applicants at random through a costlier document verification platform.

Ultimately, with little insight into which identity elements can help predict risk in a new market, Sun Finance can't customise onboarding workflows according to actual applicant risk. This challenge results in more drop-offs, increased fraud and higher acquisition costs.

3%

With Mastercard's account opening solution, Sun Finance were able to identify and reject a previously unknown segment of high-risk applicants that accounted for 3% of monthly sales.

Approach

Our solutions enabled Sun Finance to go beyond traditional data sources to gain insight into the validity and behaviour of the identity elements gathered at sign-up—name, phone, email, address and IP—by providing the risk signals and scores to more confidently identify and separate potential bad actors from good customers during the application process.

This means Sun Finance can now customise onboarding flows, offering low-risk customers a low-friction workflow. This improves the customer experience by onboarding good customers more quickly. High-risk applicants, on the other hand, are sent through a higher friction onboarding workflow or simply declined altogether.

Find the complete case study here.

Solution

The confidence our data gives Sun Finance in risk decisioning can't be underestimated, explains the company's fraud manager.

Ultimately, our solution enables Sun Finance to identify a segment of customers they can verify with significantly lower cost per verification, significantly decreasing the acquisition costs related to this step of the onboarding process.

By calling the Mastercard API early in the onboarding workflow, Sun Finance can employ this data at various stages of the customer lifecycle. Accordingly, an important piece of our solution value rests in the robust transparency of its API response. Because there's no single risk score hidden within a black box, Sun Finance can use different signals at different points in the onboarding process—including different signals for different countries, depending on performance—as well as easily shift the thresholds in its risk models.

"It's important that Mastercard Identity don't provide a single score, but also additional features that we can use in fraud prevention. We're constantly monitoring our model performance, and it's important that scores provided by third-party vendors are stable."

Kaspars Magaznieks, Fraud Manager

About us

About Mastercard Identity

Today's digital economy opens a world of opportunity for everyone everywhere to connect. Mastercard Identity securely and seamlessly connects people with merchants, banks, and businesses worldwide — enabling them to interact with confidence how, where and when they want. Powered by global identity technologies, data and insights, machine learning scores and biometrics, organizations worldwide can verify and authenticate more genuine consumers and prevent fraud in real-time. From the initial account opening through account changes – and across the entire payment transaction and fraud ecosystems, Mastercard Identity instills trust on both sides of the interaction.