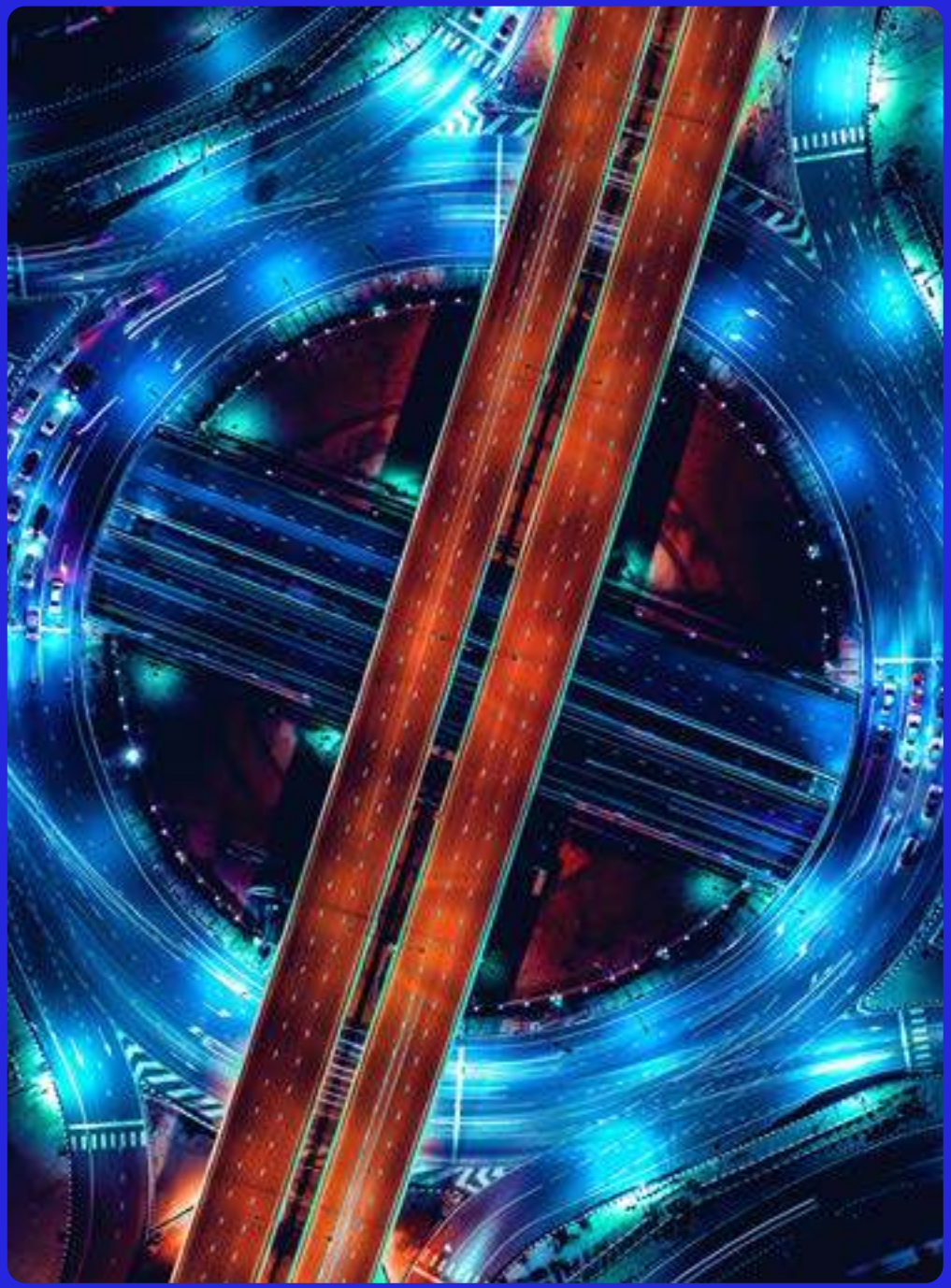
ACI Worldwide
Real-Time Payments

Achieving Digital Differentiation Through Fraud Management

Three focus areas for financial institutions that want to protect margins and increase revenue in the era of real-time payments

Start



Contents

Introduction: Differentiating Through Fraud Management

In all walks of life, the world is going digital at a quicker pace than ever before: from entertainment to transport, from fast food to even faster shopping.

The same is true in payments, which was heavily trending towards digital — and specifically real-time, as mandates proliferate around the world — even before the COVID-19 pandemic accelerated this change.

Understandably, financial institutions (FIs) have felt conflicted about how to respond. Traditional payments are a lucrative revenue stream for many organizations, while digital transactions require upfront investment, generate less revenue and — as we will see — carry increased risks. At the same time, they know that market demands for faster payments and better payment experiences are not something they can ignore.

In this eBook, we'll explore how, rather than resisting or begrudgingly accepting this transformation, FIs should consider ways to deliver premium value and differentiated experiences, including cloud deployment, by **securing and protecting digital payments through improved risk management**.

Real-Time Volumes Are Up — and So Are the Risks and Costs of Fraud

THE TASK OF COMPETING IN A REAL-TIME WORLD IS AN UNENVIABLE BALANCING ACT FOR FIs.

The biggest benefits of digital and real-time channels — **convenience, speed, broader accessibility** — are also their main vulnerabilities, and the digital world is inherently weaker than the physical one. (Safecracking is a lot of effort and not very scalable, but the digital equivalent can simultaneously attack thousands of targets with only an internet connection and free-to-download malware.)

Meanwhile, the financial impact of digital payments fraud on FIs is also greater than that of its physical counterpart. With more transactions and touchpoints to secure (vertical complexity) and more data to monitor (horizontal complexity), it's more costly to process digital payments and the margins are thinner. The losses hurt more.

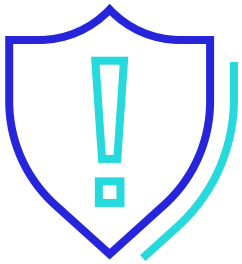
It's harder, too, to spot the bad transactions among the increased volume of genuine ones, and the time available to react to them is measured in just milliseconds.

Finally, as if that wasn't enough, there are risks with being overly protective. The expectation among consumers today is for frictionless cross-channel commerce. Throwing up barriers that slow them down is the fast-track to customer churn and market share erosion.

This Is a Critical Time for Fraud Management

AGAINST THIS BACKDROP, THE COVID-19 CRISIS HAS CREATED YET MORE FERTILE GROUND FOR FRAUD, WHILE ALSO UNDERMINING THE OPERATIONAL CAPACITY OF ISSUERS, MERCHANTS AND ACQUIRERS TO DEFEND AGAINST IT.

As even more commerce is conducted online, often through hastily transplanted or repositioned business models, we expect fraud to proliferate in the form of account takeovers, scams, friendly fraud, disputes/chargebacks and opportunistic fraud, such as lost/stolen and contactless fraud.



Therefore, it's never been more important for FIs to have strong opportunity management controls in place to close or minimize vulnerabilities, alongside the tools and processes needed to operationalize and integrate these controls within the customer experience.

Now more than ever, fraud leaders that are prepared to embrace fraud management as a competitive differentiator have an opportunity to recover lost payment revenues and capture additional market share, by developing added-value risk management services. And they have just the compelling event they need to sell it into their leadership peers and the wider organization.

Our experience shows that FIs can focus their response efforts in three core areas in order to capture the maximum upside of this potential opportunity, through increased capabilities and improved operational efficiencies (click a heading to jump to that section):

- **Focus area #1: Enhancing opportunity management and regulatory compliance through strong customer authentication (SCA)**
- **Focus area #2: Democratizing access to machine learning and leveraging the power of network intelligence**
- **Focus area #3: Pursuing relentless efficiency through robotic process automation**

Focus Area #1: Enhancing Opportunity Management and Regulatory Compliance Through SCA

Strong customer authentication (SCA) has emerged as one of the most important — and challenging — payments fraud prevention measures available to FIs today.

While it is designed to dramatically improve consumer and FI protection against unauthorized payments — which have been steadily climbing in recent years — the technical challenges of its implementation, and the potential risks to customer experience, have caused major concern among players throughout the payments ecosystem.

In Europe, incoming regulations under the EU's Second Payment Services Directive (PSD2) mean FIs are under added time pressure to solve these challenges. But SCA — in whatever form — is a global issue that strikes to the heart of creating frictionless yet safe payment experiences that consumers can trust.

Under SCA, online or card-not-present (CNP) transactions will — with some exemptions — need to be approved on the basis of two or more of the following factors:

Knowledge
A PIN, a password or the answer to a secret question

Possession
A token or a known, trusted device

Inherence
A factor inherent to the individual, such as biometrics (typically fingerprints, facial recognition or voice recognition)

Certainly, not all friction is bad. Consumers want to know they are being protected. But reports of dizzyingly high abandonment rates for online purchases resulting from strong authentication cannot be ignored.

Regulatory pressure or not, SCA is a challenge that will be relevant for many years to come. **Arguably, it's time to double down on exploring how your organization can best deploy SCA exemptions and risk-based authentication to protect the customer experience.**

Why The Time Is Now for SCA Exemptions

SCA IMPACTS MERCHANTS, ACQUIRERS, ISSUERS AND PROCESSORS IN DIFFERENT WAYS, SO THEIR CONCERNS ARE NATURALLY VARIED.

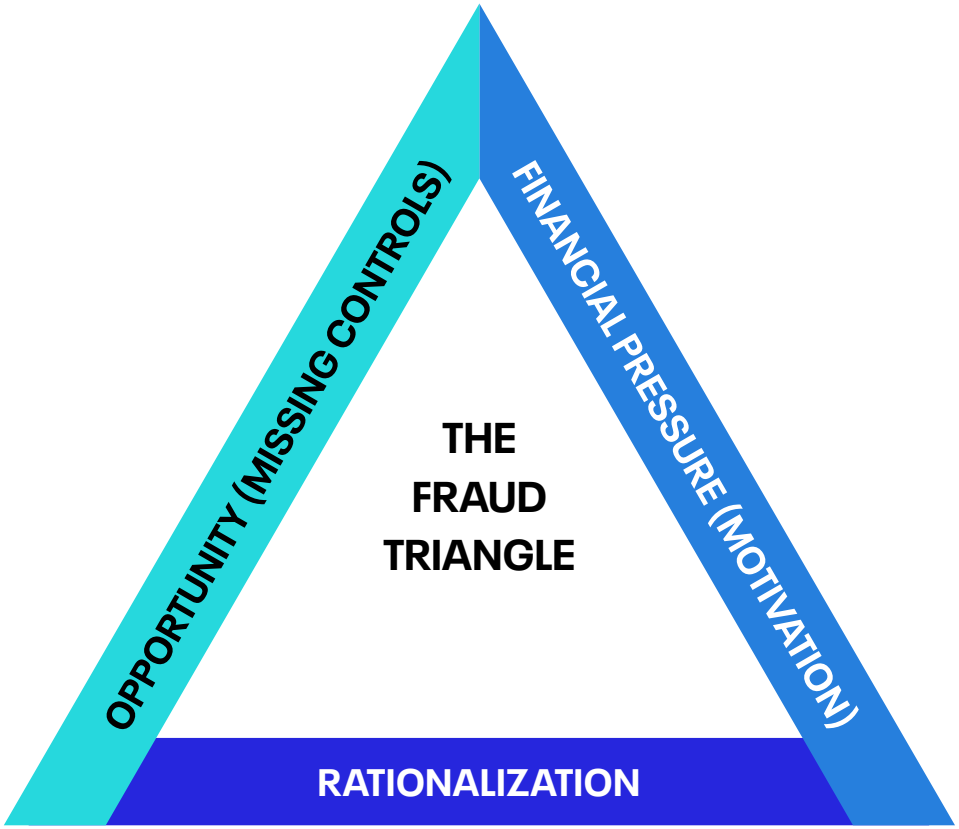
Merchants will be concerned that high abandonment rates associated with SCA will impact sales, erode customer loyalty and discourage repeat purchases.

Many issuers will be concerned about their increased fraud liability as a result of a rise in the number of merchants using 3-D Secure (this SCA protocol pushes more liability their way), at a time when many issuers are behind the curve on 3DS 2.2 adoption. Additionally, the fallout for higher abandonment rates will likely increase inbound calls (customers tend to call their bank whenever they run into obstacles), and their cards risk being pushed to the back of the wallet out of frustration with poorly implemented SCA protocols.

Of universal concern, however, is that world events are also making fraud much more likely. Pressure is growing on "The Fraud Triangle," particularly on the opportunity side that SCA is designed to protect. (See diagram on next page.)

As such, FIs should instead be looking to use this time to revisit the ways they can apply SCA now, but manage the implementation so that allowable exemptions can be applied to protect the customer experience. These have the potential to turn SCA compliance into a competitive advantage, yet many FIs have previously dismissed them as an additional layer of complexity.

Fraud and COVID-19: The Creation of the Perfect Storm



Examples:

- **Alien working environments** — e.g., newly initiated home-working/ disparate workforce
- **Rush to implement mitigating business practices to replace lost revenue** — e.g., move from brick and mortar to eCommerce without normal due diligence and controls
- **Staff shortages** — e.g., due to sickness, self-isolation
- **Reliance on temporary workforce** — due to excessive new demands on goods and services or due to staff shortages

Examples:

- Not meeting sales targets
- Job insecurity
- Loss of employment
- Threat of bankruptcy
- Gambling
- Global pandemic
- Forced closure of business
- Inability to claim from government aid packages
- No ability to see light at the end of the tunnel

Examples:

- "I had to replace lost earnings somehow"
- "I was only borrowing it"
- "I had bills to pay"
- "The banks are insured — there's no victim here"
- "The victim" will get his money back
- "I was going to lose the roof over my head"
- "I was only protecting my family"

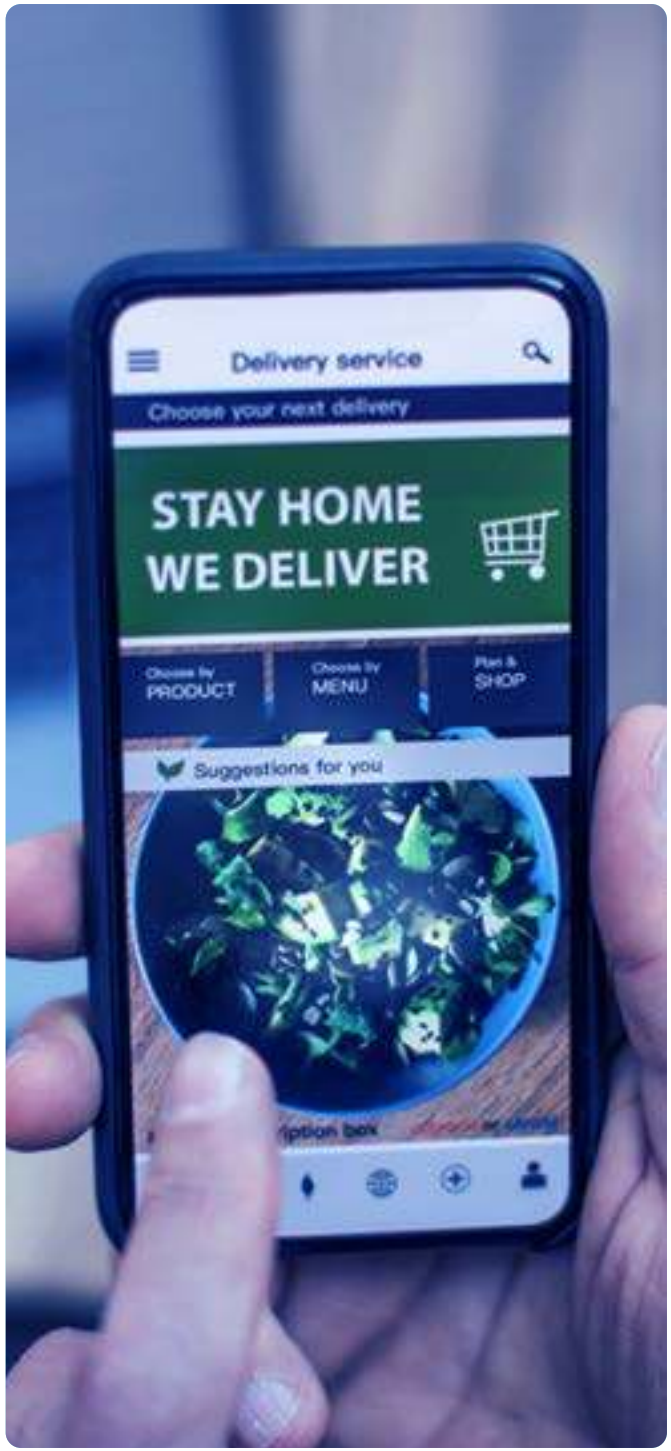
The Business Case for SCA Exemptions

ULTIMATELY, SCA AND EXEMPTIONS ARE A GOOD THING AND THE MOST SUCCESSFUL FIs IN THIS AREA WILL DIFFERENTIATE THROUGH THEIR ABILITY TO APPLY THE MAXIMUM POSSIBLE EXEMPTIONS THEY CAN AND REAP THE REWARDS OF IMPROVED CUSTOMER EXPERIENCE AND, IN TURN, CUSTOMER LOYALTY.

In not doing so, acquirers risk creating a poor customer experience arising from SCA that will mean higher cart abandonment and loss of market share; likewise, issuers could find their cards pushed to the back of the wallet in favor of competitors that offer less friction.

Instead, merchant acquirers can create opportunities to increase revenue by charging for exemption services. This would be justified by reduced abandonments, increased customer loyalty, reduced fraud (based on the effectiveness of their risk-based authentication) and reduced inbound calls when customers have issues with their transactions.

Issuers and issuer processors can be similarly ambitious in the hunt for increased revenue. Providing a 3DS service to issuers (processors only) that promised increased transactions through reduced abandonment rates would mean more interchange revenue and greater customer loyalty. There are opportunities too around net interest income on credit card transactions, reduced inbound calls from customers unable to complete or failing authentication, and reduced fraud through improved risk assessments.



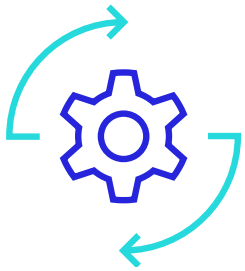
Learn More: Applying SCA Exemptions

PSD2 allows for exemptions from SCA based on the level of risk, transaction value, recurrence and the payments channel. However, applying them successfully requires split-second decision making as to whether or not a transaction requires SCA.

To discover more about applying SCA exemptions to create a competitive advantage, please take a look at our webinar **Implementing strong customer authentication (SCA) exemptions** and accompanying **eBook**.

Focus Area #2: Democratizing Access to Machine Learning and Leveraging the Power of Network Intelligence

For all the upsides of digital payments in terms of better, faster experiences for customers, there's no avoiding the increased levels of associated risk for FIs. When payments happen in real time, the window for fraud detection is reduced to milliseconds and the likelihood of recovering fraudulent payments is far lower than with traditional methods. Essentially, as payments get faster, so too does fraud — and when it's gone, it's gone.



Furthermore, as the volume and variety of digital payments surge, so too do the volume and variety of data generated by those payments. Geo-location information, behavioral clues and biometrics provide a wealth of intelligence for FIs — but only if they can make sense of the deluge.

As such, machine learning has emerged as an essential complementary tool for detecting the fraudulent payments among the many thousands or millions of genuine ones made every day. It is the only way for FIs to operate at the speed and scale required to authenticate genuine payments, catch fraud as it happens, reduce the volume of false positives and improve the time it takes to react to them when they do occur.

Yet to be truly effective in the fight against fraud, **machine learning solutions must be agile enough to be developed**, **tested**, **deployed** and **updated**, as either new threats emerge, or as existing ones become better understood. And they must have access to an industry-, region- or market-wide view of possible threats — not just an internal one — because their decision-making performance improves as they interact with more data patterns.

Democratizing Access to Machine Learning

TO ASSIST FIs WITH THE FIRST OF THESE CHALLENGES, TOOLS SUCH AS ACI's MODEL GENERATOR DEMOCRATIZE ACCESS TO MACHINE LEARNING BY ENABLING NON-SPECIALISTS TO BUILD, TEST AND DEPLOY MODELS IN MINUTES.

They do this by abstracting away from users the complex math that lies behind these models, replacing it with an intuitive interface for drag-and-drop model building using the "features" of fraud as building blocks. In bringing machine learning to an organization's in-house data and fraud expertise — as opposed to taking that data and expertise to a machine learning specialist — these solutions accelerate the time to market of fraud-fighting applications.

THE BENEFITS OF DEMOCRATIZED MACHINE LEARNING

- Resolve the burden and regulatory risks for attempting to extrapolate and submit data externally.
- Enhance operational efficiency through improved false positive rates and detection rates.
- Reduce fraud losses through faster and improved detection and preparation for future fraud threats.
- Work with live data without risk of hindering performance.
- Create as many models as needed and focus on different channels and typologies.
- Improve consumer experience ensuring fraud is declined/identified and genuine transactions are approved.

As FIs become aware of new fraud risks, additional features can easily be added to the models and the weight of evidence scoring adjusted accordingly, ensuring banks' defenses keep pace with emerging risks. This can even take place automatically, through adaptive machine learning solutions that respond to analyst-applied "markers" for potential fraud and adjust models accordingly.

This promises to transform the way FIs use machine learning by allowing them to adopt a business-led approach, which offers greater ownership and control of their fraud detection strategy. It empowers them to act self-sufficiently without the costs, risks and time of involving third parties in AI implementations, and — importantly for compliance — it promotes better explainability of the solution's outcomes.

Further Reading: Everlink Payment Services Accelerates Machine Learning Deployments

Discover how democratized access to machine learning with ACI's model generator offering helped Canada's Everlink Payment Services accelerate operationalization of these solutions, while balancing loss mitigation, client experience and operating efficiency.

Read the Case Study

The Power of Network Intelligence

INDIVIDUAL BANKS ALREADY HAVE ACCESS TO A WEALTH OF DATA WITH WHICH TO DEVELOP MACHINE LEARNING SOLUTIONS FOR FRAUD DETECTION AND PREVENTION.

However, when the intelligence gleaned from that data is shared across institutions, it has the potential to create a complex and varied intelligence network that can introduce more context to every machine learning decision. This exponentially increases its effectiveness.

Network intelligence empowers unprecedented collaboration in the fight against fraud. By harnessing the power of the community to increase threat visibility, and distributing enhanced detection and prevention capabilities back through the community, it creates a powerful jurisdiction- or network-level deterrent to fraud.

Network intelligence takes the features of machine learning models deployed by individual participating organizations and sends them out to a central repository in meta data format. That could be a central infrastructure (CI) or an organization to which the individual participating FIs belong (either as members or are connected to) where they can be tested against the community view for their effectiveness. (See diagram on next page.)

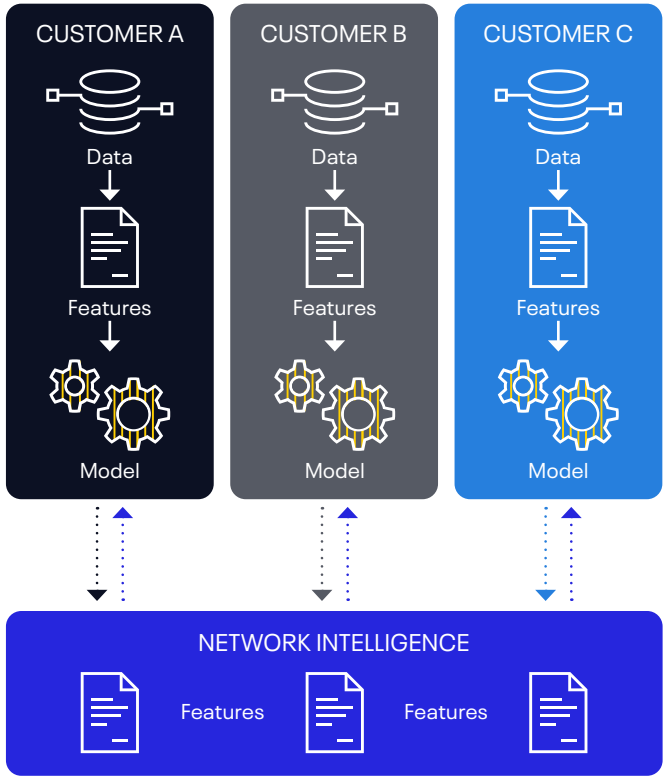
How Network Intelligence Works

ONCE TESTED, THESE FEATURES ARE THEN MADE AVAILABLE TO THE REST OF THE COMMUNITY FOR MEMBERS TO AGGREGATE WITH THEIR OWN MODELS OR TO BUILD UPON AS NEEDED.

This enables a **hybrid machine learning** and risk scoring approach, where FIs can create models that combine the community view with their own proprietary view.

Every organization's view of risk is unique, so once community features are imported they can quickly be tested against internal data to recalculate risk scores locally. A feature that is judged by the community as a whole to be a weak indicator of fraud, may be a stronger indicator for a specific organization — and vice versa. But by combining community features or scores with local ones, FIs can benefit from the best of both worlds in a way that no other solution offers.

NETWORK INTELLIGENCE EMPOWERS UNPRECEDENTED COLLABORATION AMONG FIs



The result is increased efficiency and unrivaled flexibility when building out a machine-learning-led fraud detection strategy.

Furthermore, unlike a consortium approach, which overemphasizes its largest members' experiences of fraud, members can access the benefits of a **network intelligence** community on their terms. The biggest contributor doesn't rule the community models and risk scoring criteria.

Overall, **network intelligence** is set to be a game changer in the use of machine learning to fight payments fraud thanks to its power to improve detection of emerging threats through a scaled-up "early-heads-up" approach to feature calculation and contribution.

Network Intelligence Is a Shared Compliance

THE NETWORK INTELLIGENCE APPROACH HAS THE ADDED BENEFIT OF ALLOWING REGULATORS AND CI OWNERS TO UNDERSTAND THE WIDER FRAUD ENVIRONMENT WITH PRECISION, EMPOWERING THEM TO ACT ON NEW AND EMERGING THREATS BEFORE CLUSTERS BECOME ENDEMIC FINANCIAL CRIME RISKS.

Trends specific to organizations can be tracked and understood at any level required by a regulator, enhancing efforts to combat fraud beyond payments, such as money laundering or identity theft. Furthermore, CIs can choose to prescribe both the contributing data and time periods to ensure data consistency across the intelligence network.

This can reduce the costs of compliance too for member organizations. First, it resolves the burden and regulatory risks for attempting to extrapolate and submit data externally. Second, if a CI mandates that organizations deploy a particular model, that model can be easily distributed and then run concurrently with their own models. Indeed, an unlimited number of models can be run and tested side by side on live data without the risk of hindering performance. Suddenly, intelligence sharing to mitigate fraud using machine learning becomes easy with the use of ACI's democratized **network intelligence** offering.

Focus Area #3: Pursuing Relentless Efficiency Through Robotic Process Automation

Once organizations have deployed a future-proofed SCA compliance strategy and democratized, **network-intelligence-led**, machine learning capabilities, they need to turn their attention to increasing operational efficiency.

Even with these strategies and solutions in place, the forecasted increase in digital transaction volumes means there's no avoiding the fact that more genuine customers will be impacted by fraud prevention measures, potentially increasing operational overheads for servicing these customers.

To reduce the time to react to these situations when they occur, and preserve the customer experience in a cost-effective way, FIs need to find a way to do more with their existing resources. That means they need **responsive**, **automated** and **context-oriented two-way communications solutions**. The only other alternative is to hire more people, which is often cost-prohibitive and almost impossible in today's environment. **Increasingly, FIs are turning to the emerging field of robotic process automation to make this happen**.

WHAT IS ROBOTIC PROCESS AUTOMATION?

Robotic process automation automates business processes using technology — mainly software — governed by business logic and structured inputs. Robotic process automation tools allow businesses to **automatically respond to data**, **events** and **interactions to process transactions**, **trigger customer outreach** or **communicate** with other digital systems.

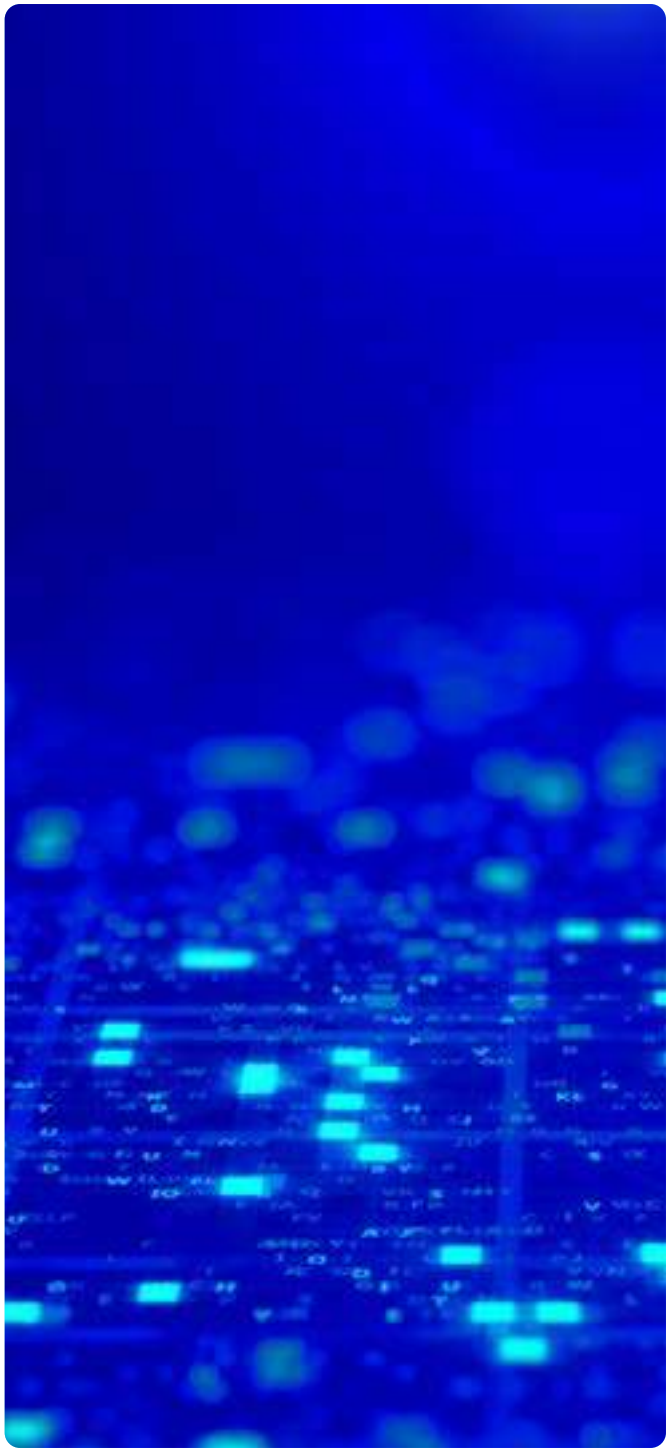
The Need For Robotic Process Automation

AUTOMATED FRAUD DETECTION AND SCA COMPLIANCE SOLUTIONS ARE ABLE TO MONITOR MORE TRANSACTIONS MORE CLOSELY AND AT A GREATER VELOCITY THAN ANY HUMAN COULD EVER HOPE TO ACHIEVE.

This also means there's more scope for them to flag activity that deviates from the norm but isn't necessarily suspicious. For example, when a customer logs in using a different device, it's less likely to be unauthorized access and more likely that they've upgraded their phone. Nevertheless, it needs verifying.

To avoid overwhelming already stretched human resources, such as call center and support staff, and introducing more friction for the customer, these non-financial transaction scenarios — and thousands like them — need to be digitized, automated and contextualized wherever possible.

This is a complex challenge, but getting it right promises to provide an additional layer of competitive differentiation for FIs. It opens the opportunity to provide greater fraud coverage and more seamless experiences that can be applied consistently to an organization's entire customer base. All without additional headcount in either the fraud shop or service centers.



The Next Frontier In Customer Centricity

TO ADDRESS THIS CHALLENGE, FIs NEED AUTOMATED TWO-WAY COMMUNICATIONS SOLUTIONS FROM TRUSTED PROVIDERS, WHICH CAN INTEGRATE SEAMLESSLY WITH THEIR FIRST- AND SECOND-ORDER MONITORING SOLUTIONS FOR FRAUD MANAGEMENT.

When the fraud management solution spots anomalous activity and recommends further verification, it can hand that off to the communications solution to initiate automated and predefined communications workflows based on the contextual inferences made from the data held on that customer.

In this way, robotic process automation allows for banks to truly build their fraud management strategy around the customer, and not around their own channels or other organizational factors that may have little bearing on the customer's needs.

It also serves to ensure that specialist human resources like fraud analysts are free to focus only on the activity that's deemed the highest risk and therefore the highest priority, which machines cannot — and should not — be left to handle.

Furthermore, robotic process automation improves the application of fraud management frameworks and policies to boost risk mitigation (both in terms of fraud and reputational risks) and enhance compliance. It forces organizations to clearly define what their policies are, and the practical steps required to enforce them. And by removing the need for human intervention in the majority of cases, rules and procedures will rarely be bypassed — machines will always follow rules.

ACI Worldwide: A Solution Framework for Differentiating Through Fraud Management

Clearly, widespread optimization work is necessary for any fraud team to be able to profitably protect digital payments from fraud through precision detection, at speed, and in line with their unique fraud coverage or segmentation strategies. And this work needs to be correctly balanced with minimizing the poor customer experience associated with SCA and falsely blocked genuine activity.

That means FIs need solutions that empower them to apply controls in the way that works for them, all wrapped up in processes and tools that increase their time to react to both false positives and genuine fraud attempts.

The ACI solution framework enables FIs to meet these challenges head on, from deploying a powerful and accessible fraud management engine that leverages machine learning, to detecting more fraud than ever before, to automating two-way communications solutions for creating winning customer experiences.

Additionally, ACI has partnered with Microsoft to deliver its solution in the Microsoft Azure cloud. This gives FIs the power to quickly react to new market pressures (such as COVID-19) and deploy a fraud solution in a matter of hours.

Learn More Here

ACI Worldwide
Real-Time Payments

ACI Worldwide is a global software company that provides mission-critical real-time payment solutions to corporations. Customers use our proven, scalable and secure solutions to process and manage digital payments, enable omni-commerce payments, present and process bill payments, and manage fraud and risk. We combine our global footprint with local presence to drive the real-time digital transformation of payments and commerce.

LEARN MORE

www.aciworldwide.com

@ACI_Worldwide

contact@aciworldwide.com

Americas +1 402 390 7600
Asia Pacific +65 6334 4843
Europe, Middle East, Africa +44 (0) 1923 816393

ABR1135 04-21