ACI Worldwide
Real-Time Payments

Expanding the Horizons of Fraud Detection

How the network intelligence approach to machine learning is driving unprecedented collaboration in the fight against payments fraud

Start

The Need for Network Intelligence in a Real-Time World

DIGITAL PAYMENTS, AND ESPECIALLY REAL-TIME ONES, HAVE LED TO AN EXPONENTIAL INCREASE IN THE COMPLEXITY OF FRAUD DETECTION FOR FINANCIAL INSTITUTIONS (FIs).

The growing diversity of payment types, soaring transaction volumes and their increasing speed (as seen in ACI's Prime Time for Real-Time Report) mean more data to monitor and less time to do it. While that potentially means more insight into what fraud looks like for FIs, the data deluge has also diluted the strength of any individual signal as a fraud indicator. The needles have become smaller as the haystack has grown.

Additionally, the global pandemic of 2020 exposed an unexpected challenge for many banking fraud teams—ensuring their fraud solutions keep pace when attacks have accelerated beyond recognition.

To tell the genuine from the fraudulent, FIs must make an assessment of risk based on a combination of diverse and changeable data "features," such as location, device type or transaction history. And they must do it in milliseconds.

Other factors count against FIs, too. Recoverability is much lower when payments are sent instantly. And, with customer experience so crucial in the age of digital transformation, false positives come with their own risks when the competition is only a click away.

Given these challenges, machine learning has become the default fraud detection and prevention technology for many FIs. Able to process and learn from data far faster than humans, it reduces the noise surrounding digital transactions to enable FIs to build efficient, rules-based fraud prevention strategies. What's more, we have seen that cloud-based systems have proven their mettle when banks needed to quickly pivot, as in the case of COVID-19.

Nevertheless, machine learning has its limitations.

Machine Learning is Good, But It's Not Perfect

SINCE MACHINE LEARNING SYSTEMS ARE ONLY AS GOOD AS THE DATA THEY WORK WITH, THEY MUST BE EXPOSED TO THE WIDEST POSSIBLE VIEW OF RISK—IN REAL TIME—WHICH REQUIRES ACCESS TO DATA FROM INSIDE AND OUTSIDE OF THE ORGANIZATION.

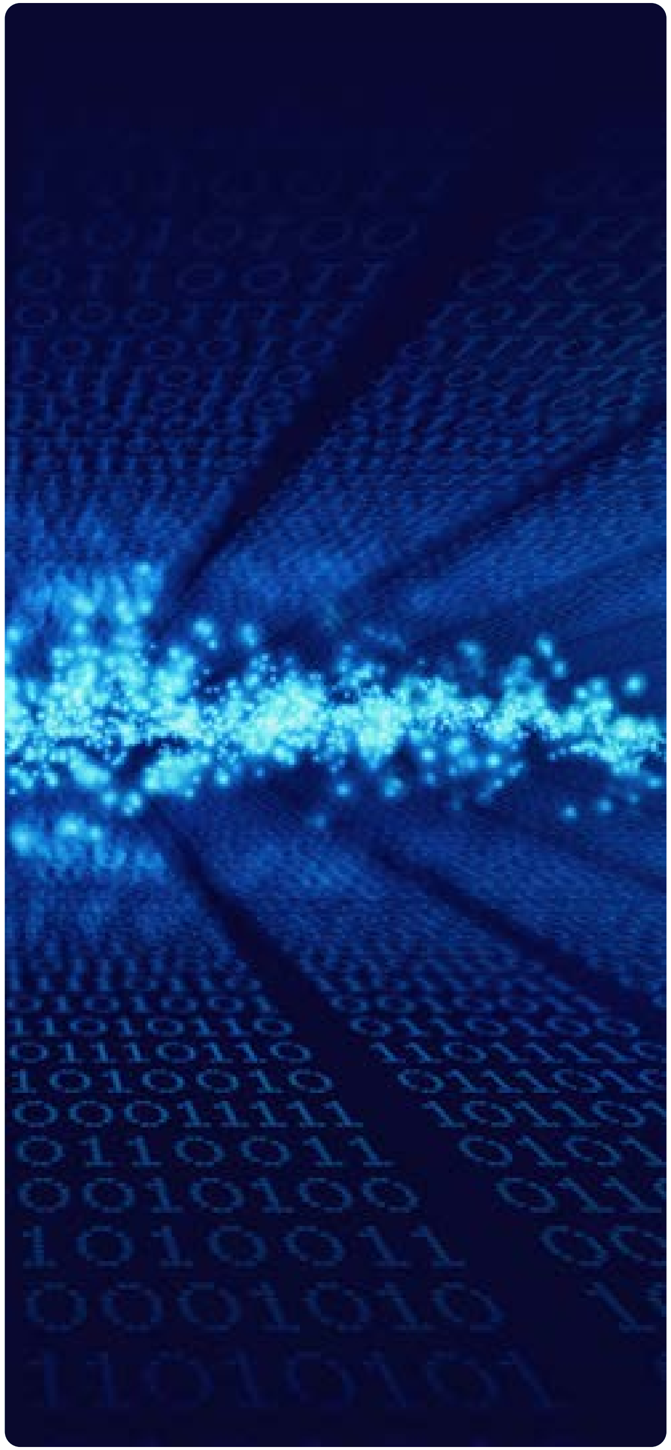
And they must be agile and adaptable enough such that changes can be made as new threats emerge, as evidenced by the rapid rise of COVID-19-related fraud. That means machine learning capabilities must be democratized so that analysts are the ones with their hands on the levers—not data scientists.

This matters because detecting and preventing payments fraud is a perennial game of cat and mouse. Once criminals spy an opportunity, they maximize its exploitation, only moving on once FIs catch up and close the vulnerability. When they find another opening, the process begins again. Payments fraud is also a systemic threat. It risks undermining trust in new payment types and services—ultimately limiting adoption and stifling innovation—and it transcends organizational and national boundaries.

As such, FIs must take a similarly wide view with their payment risk strategies to secure digital payments and maintain consumer confidence—and to reduce or eliminate the mouse's head start on the cat. Without it, their understanding of risk will be limited only to threats they've directly experienced, handing a potentially decisive advantage to the criminals.

The community approach to payments fraud risk modeling has emerged as a leading way to meet these requirements. It is pushing new horizons of collaboration between FIs in the fight against payments fraud, and ACI is leading the way with its network intelligence capabilities (part of ACI's model generator feature).

This community approach is further bolstered by ACI's partnership with Microsoft, which enables banks to rapidly launch their fraud solution in the cloud in a matter of hours, versus several weeks for an on-premise deployment. Combined, banks can now quickly upgrade customer-facing software and adapt solutions to eliminate fraud.



Understanding the Power of the Community

FIs HAVE A LONG-HELD TRADITION OF PUTTING ASIDE THEIR COMPETITIVE INSTINCTS TO COLLABORATE IN THE FIGHT AGAINST FRAUD.

But traditional consortium-type efforts have always had the disadvantage of taking a one-size-fits-all view, where the largest players disproportionately influence the group's outcomes. They're also characterized by a slow turnaround—relative to the lightning fast requirements of the digital age—in terms of collecting data, building it up into a usable model and distributing it to the rest of the group.

A network intelligence community, on the other hand, facilitates real-time information sharing of new and emerging risks. Through consistent and transparent information sharing, localized threats can be quickly understood before they become endemic. And all members are served equally because they can engage on the terms that work for them, in both directions (contributing insights and adopting the community findings), meaning the biggest contributor doesn't rule the models and scoring.

A community approach also allows regulators and central infrastructures (CIs) to be active in the community, expanding their role beyond just supervision. This enables vital end-to-end collaboration in the development of regulations and their compliance.

In short, fraudsters thrive on uncertainty and gaps in knowledge. The community reduces both by creating a network or jurisdiction deterrent and defense, with every player engaged in real time.

Empowering Unprecedented Collaboration

NETWORK INTELLIGENCE HERALDS AN ERA OF UNPRECEDENTED COLLABORATION IN THE FIGHT AGAINST PAYMENTS FRAUD (*FIGURE 1*), TEARING DOWN THE LAST REMAINING BARRIERS TO GENUINE INDUSTRY-WIDE FRAUD DETECTION AND PREVENTION.

By enabling the community to share, in real time and in meta-data format, their fraud models in their composite features (along with key performance data supporting their efficacy), the community can share more information at lower risk. Automatically stripping the meta data of any identifiable information resolves the burden and regulatory risks around attempting to extrapolate and submit data externally.

While the community's central body, perhaps a CI, controls quality and oversight by pre-aggregating the data to form consistency in data and flow across members, it does not decide which models the group adopts—the community does. Furthermore, members can adopt, adapt or combine features with their own models however they see fit. In this way, participants can integrate proven model features into their own customized adaptive machine learning strategies, enabling a hybrid approach to model creation and risk scoring.

The result is that the community organically creates informative, non-redundant and contextually meaningful data features, focused on individual members' requirements. Ultimately, network intelligence allows FIs to share more information, faster, while better policing the quality of information they receive in return.

This is radically different to other collaboration models that rely on members to contribute trends to a central body, which then decides how to build out a single consortium model based on those trends. Consortium members knowledge. The community reduces both by creating a network or jurisdiction deterrent and defense, with every player engaged in real time.

NETWORK INTELLIGENCE EMPOWERS UNPRECEDENTED COLLABORATION AMONG FIs

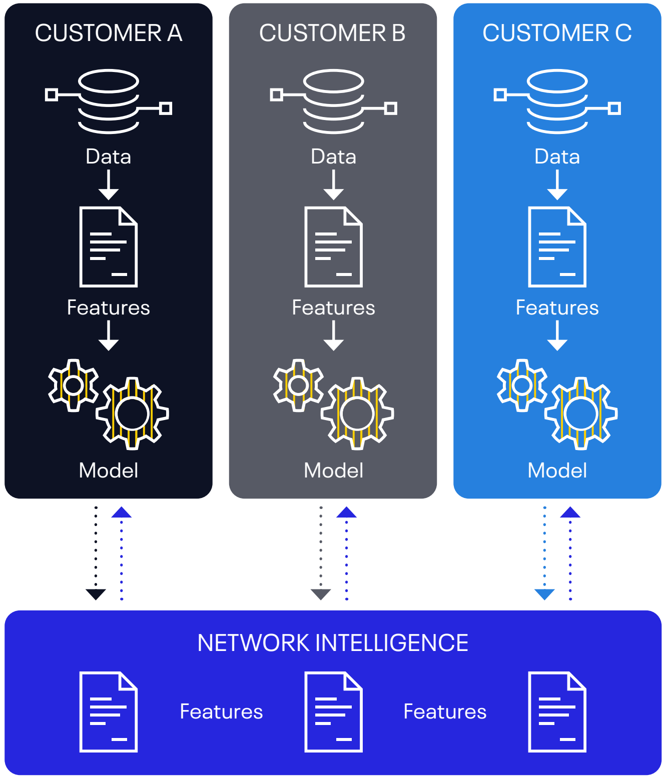


FIGURE 1

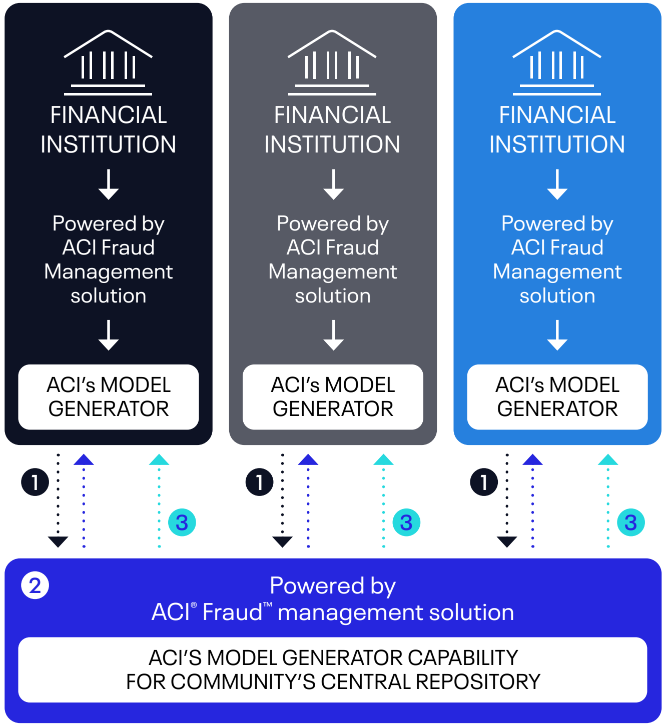
Use Case: Three Steps to Network Intelligence

NETWORK INTELLIGENCE SIMPLIFIES FRAUD DETECTION BY LEVERAGING COMMON FEATURES AMONG THE COMMUNITY, MAKING IT LESS OF AN INVESTMENT TO DEPLOY NEW FRAUD ATTRIBUTES OR FEATURES TO MACHINE LEARNING MODELS (*FIGURE 2*).

Key benefits of this approach include:

- Democratization of machine learning through intuitive UIs for validating and automatically applying community contributions, accelerating time to value
- Overall improved detection through a "leading indicators" approach to feature calculation and contribution, enabling a "champion and challenger" approach to risk scoring
- A hybrid approach to machine learning and risk scoring, which enables increased efficiency and unrivaled flexibility.
- No limitations on concurrent number or type of models
- Ability to work with live data without risk of hindering performance

THREE STEPS TO NETWORK INTELLIGENCE



FINANCIAL INSTITUTION
Powered by ACI Fraud Management solution
ACI's MODEL GENERATOR
FINANCIAL INSTITUTION
Powered by ACI Fraud Management solution
ACI's MODEL GENERATOR
FINANCIAL INSTITUTION
Powered by ACI Fraud Management solution
ACI's MODEL GENERATOR
1
3
1
3
1
3
2
Powered by
ACI® Fraud™ management solution
ACI'S MODEL GENERATOR CAPABILITY
FOR COMMUNITY'S CENTRAL REPOSITORY

FIGURE 2

1 Members receive feature definitions from the community's central repository, and feedback their local risk scores.

2 This information is aggregated to calculate new feature values, which are shared back through the community.

3 Community members decide whether to adopt or adapt new features, based on their unique fraud strategy.

The Path to Value with Network Intelligence

AS PAYMENT CHANNELS MULTIPLY, TRANSACTIONS GET FASTER AND PAYMENT MESSAGING FORMATS EVOLVE TO CONTAIN EVER MORE DATA, MACHINE LEARNING-BASED FRAUD DETECTION AND PREVENTION STRATEGIES ALSO NEED TO EVOLVE.

They must adapt to bring together richer data sets from inside and outside the organization to enhance scoring. This is crucial for maintaining the customer experience, by reducing false positives, to limit fraud losses and bolster compliance.

In this context, network intelligence offers accelerated paths to value from machine learning for key players in the payments ecosystem.

Exponential Increase in Machine Learning Effectiveness for FIs

Individual FIs already carry a wealth of customer data with which they can build resilient, agile fraud defenses. But by sharing that data across institutions, they can create a complex and varied intelligence network that introduces more context to every machine learning decision. This exponentially increases its effectiveness.

ACI's network intelligence enables the community to share unlimited fraud features, improving network-wide fraud detection rates and strengthening coverage of new and emerging threats. As a result, FIs can become more assertive in the fight against fraud — ultimately providing their customers with greater protection.

Enhanced Solution Portfolio for Processors

Network intelligence capabilities can be leveraged by processors to provide value-added services to their network of customers through, for example, community risk scores as a service. This offers a sure path to competitive differentiation in a crowded market where margins are being squeezed by growing volumes of digital transactions.

Smarter Policy and Regulation Development for CI Owners

A wider view of what's happening in their environment can better inform CIs' development of policies and regulations, either to meet emerging or persistent threats or improve the consistency of compliance.

For example, they can develop a community- wide view of the specific challenges members are facing, such as problems across online banking or with IP addresses originating from outside of their jurisdiction. This allows them to build a clearer story around the threats organizations are facing, ensuring regulations are based on a consistent and formalized view of their environments.

Discover More: ACI® Fraud Management™ Solution

The need to build out, deploy and constantly adapt advanced predictive machine learning models is in demand more now than ever before.

ACI's network intelligence solution builds on ACI's model generator framework, which works in conjunction with ACI Proactive Risk Manager™, part of the ACI Fraud Management solution, to empower fraud analysts to develop, test and launch their own adaptive machine learning models within hours.

This allows FIs to reduce their reliance on specialized resources and adopt a business-led machine learning strategy to match today's fast-paced, 24/7 fight against fraud. ACI's model generator capabilities support the complete model development process, allowing for easy access to examine and analyze data, calculate scenarios and document key modeling steps. The ability to build, evaluate and deploy models is unlimited.

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