



Whitepaper

Network Intelligence at Scale: Mastering Real-Time A2A Fraud Prevention

feedzai[↑]



Table of contents

Executive Summary 3

The Evolving Challenges of A2A Payments

 1: The A2A Scam Crisis 4

 2: Regulators Increasingly Demand Change 5

 3: The Limits of Siloed Defenses 6

The Solution: Network Intelligence at Scale 7

How Mastercard's Consumer Fraud Risk (CFR) Works 9

Real-World Impact (UK Case Study) 11

Strategic Benefits of the Feedzai-Mastercard Partnership 13



Executive Summary

Institutions leveraging Mastercard's Consumer Fraud Risk (CFR) solution are already seeing tangible benefits in combatting fraud. Early deployments in the UK demonstrate CFR can assist with intercepting Account-to-Account (A2A) scams in real time. Stopping fraud and scams before the funds leave the victim's account helps financial institutions reduce consumer losses, materially lower operational costs and, most importantly, preserve Customer Trust.

The urgency is clear: scams are growing in scale and sophistication, with criminals increasingly exploiting instant payment rails and emerging technologies to steal funds in seconds.

CFR is being developed for global markets in collaboration with Feedzai to bring this capability to scale. By combining Mastercard's global footprint and multi-rail reach with Feedzai's real-time AI decisioning, institutions gain real-time risk scoring for both sender and receiver, providing a unified view of risk before transactions occur.



The Evolving Challenges of A2A Payments

1 The A2A Scam Crisis

The **scope and speed** of today's scams demand an intelligence-driven defense. Criminals exploit digital banking and trust: they craft deepfake websites and social-engineering schemes to manipulate customers into authorizing transfers. Faster payment adoption multiplies the attack surface. The Global Anti-Scam Alliance reports that more than 50% of people encounter a scam weekly¹.

Key industry trends fueling A2A scam risk include:

- ➔ **Technology-driven Scale:** AI tools lower barriers for fraud. Emerging GenAI voice, text, and bots enable criminals to craft convincing scams at scale.
- ➔ **Growing Real-time Payments:** Real-time payments continue to expand rapidly. Globally, real time payments are projected to surge at a compound annual growth rate (CAGR) of 16.7 percent, reaching 575.1 billion transactions by 2028.²
- ➔ **Human Vulnerability and Low Awareness:** Many victims assume authorized payments are safe. Fraudsters exploit urgency, authority, and emotional manipulation to pressure victims into approving transfers before they can verify the request. While governments, regulators, and banks are expanding awareness campaigns, the scale and sophistication of modern scams mean education alone has not kept pace with the threat.

¹ <https://www.feedzai.com/pressrelease/mastercard-and-feedzai-join-forces-to-protect-consumers-and-businesses-from-scams/#:~:text=As%20payments%20continue%20to%20evolve%2C,point%20the%20transaction%20is%20made>

² Global Real-Time Payments Growth "Sustainable" As New Use Cases Push Transactions to Record Highs – ACI Worldwide Report | ACI Worldwide



2

Regulators Increasingly Demand Change

Worldwide, regulators are reshaping the liability model for payment fraud, shifting **responsibility away from victims and toward financial institutions and service providers** through a mix of **mandatory reimbursement rules and shared-responsibility frameworks**.

In the **United Kingdom**, for example, the Payment Systems Regulator's new rules require payment service providers to reimburse victims of Authorized Push Payment (APP) fraud up to a set cap. Under this new regulation framework, sending and receiving institutions share the reimbursement cost – creating stronger incentives for enhanced fraud detection and faster intervention, unless the customer has acted with gross negligence.

Meanwhile, the **European Union** is progressing Payment Services Regulation proposals to extend refund rights for victims of certain fraud types and to clarify PSP obligations, reflecting a trend toward reinforcing institutional accountability for fraud losses.

Australia, for instance, has introduced one of the world's most comprehensive scam prevention and shared liability frameworks, known as the Scams Prevention Framework (SPF), but with a different model than the UK or EU. Instead of mandating automatic reimbursements, Australia has built a regime where banks, telcos, and digital platforms share responsibility, obligations, and potential liability, depending on whether they took "reasonable steps" to prevent scams.

In **Singapore**, the Shared Responsibility Framework (SRF) allocates liability among financial institutions, telecommunications companies, and consumers based on whether each party met its anti-scam duties, reinforcing accountability beyond just financial institutions.

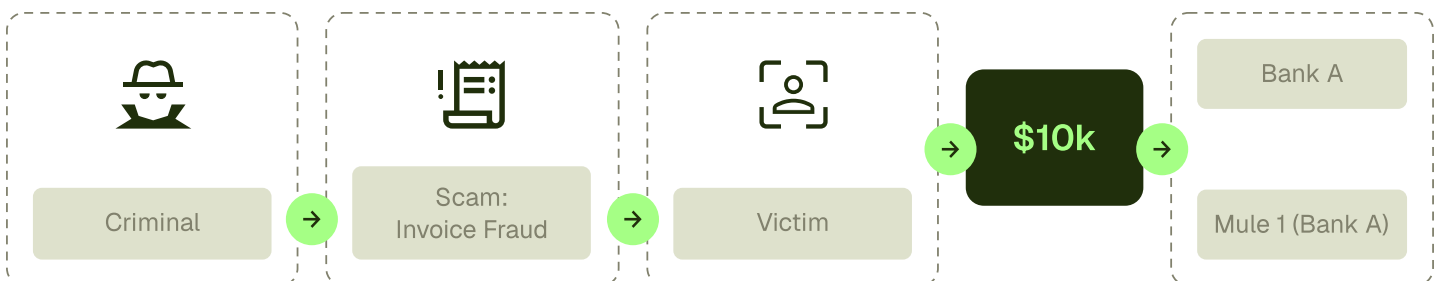
Additionally, in the **Philippines**, the passage of the Anti-Financial Account Scamming Act (AFASA) has introduced criminal penalties for organized financial account scamming and imposes new prevention, information sharing, and victim protection duties on regulated institutions.

These diverse regulatory approaches underscore the broader trend to improve protection for consumers and to compel industry stakeholders to enhance fraud prevention and control measures.



3 The Limits of Siloed Defenses

Because detection systems don't by default share cross-bank intelligence, criminals exploit the gaps. In this example, a fraudster sends a fake \$10,000 invoice and the victim transfers the money. The payment lands in an account at Bank A that belongs to the criminal crew's first money mule.



Adding to this challenge, when regulation requires financial institutions to reimburse the victims, every missed scam becomes a direct financial hit.

The shortcomings of siloed systems include:

- ➔ **Limited Visibility:** Mule accounts spread over the entire financial ecosystem, yet each bank might only detect its own individual risk.
- ➔ **Static Rules:** Pre-set rules (like account limits or watchlists) are based on past patterns and can't keep up with new or evolving scam tactics. As scams become more sophisticated, manual reviews take too long and cannot scale to billions of real-time payments.
- ➔ **Reactive Responses:** After-the-fact investigations recover only pennies on the dollar. Financial institutions lose not only stolen funds but also incur reimbursement costs under new laws. In addition, financial institutions risk eroding customer trust and ultimately losing clients.
- ➔ **No Shared Learning Loop:** Each bank identifies and relearns the same fraud patterns in isolation. Without shared intelligence, insights do not compound, preventing the ecosystem from collectively adapting as attack patterns evolve.

In short, siloed defenses leave "blind spots" that fraudsters exploit. A networked, data-sharing approach is needed to create a best-in-class defense ecosystem.



The Solution: Network Intelligence at Scale

Financial institutions must **augment their current risk strategies** by incorporating industry-wide fraud indicators. **Mastercard's Consumer Fraud Risk solution (powered by Feedzai)** serves as the leading example of this approach.

CFR addresses the core limitation of siloed fraud defenses by applying network-scale intelligence to A2A payments. Instead of relying on a single institution's partial view, CFR aggregates signals across financial institutions and payment rails, making it both rail-agnostic and effective for helping to detect highly complex scams and mule activity.

This shared view is continuously strengthened through confirmed outcomes across the network, ensuring detection evolves in step with criminal behavior and can be deployed rapidly without lengthy historical data builds.

This architecture translates directly into measurable business and regulatory impact. CFR helps institutions to intervene before funds leave the account, reducing reimbursed losses while improving operational efficiency and customer trust. Specifically, it helps financial institutions to:

- ➔ Stop fraud at the point of payment by identifying high-risk recipients and scam intent in real time.
- ➔ Reduce false positives and investigation effort through network-informed risk scoring.
- ➔ Leverage collective intelligence: risk signals discovered in one market or rail can inform and accelerate the creation of localized models in other markets.

Together, these capabilities position CFR as a foundational layer for proactive and collaborative fraud prevention across modern payment networks.

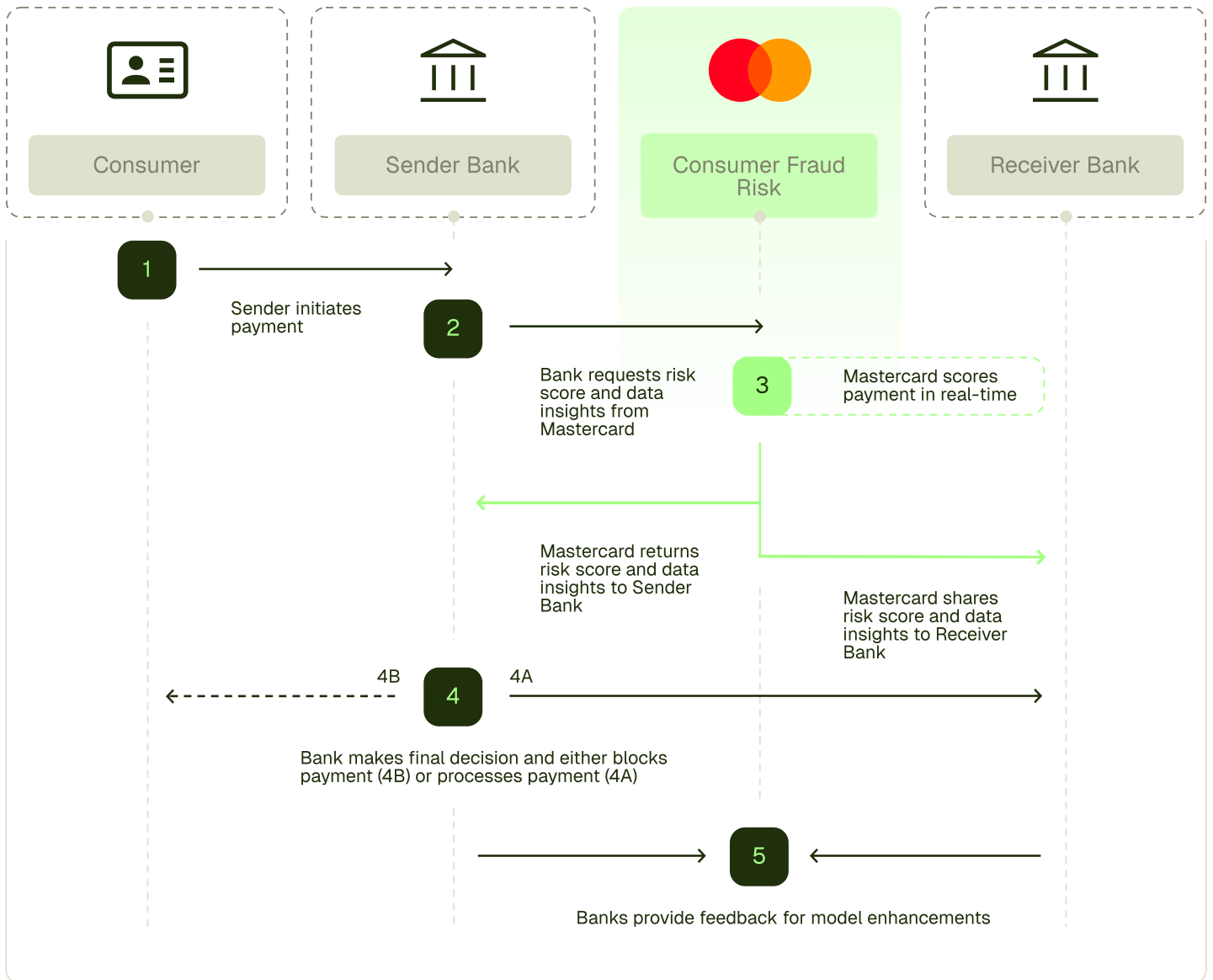


“Scams are rapidly increasing in sophistication requiring a multi layered data-driven solution, delivered in real-time. Mastercard’s Consumer Fraud Risk – a first-of-its kind, global solution, provides unrivalled network intelligence to some of the world’s leading financial institutions, stopping fraudsters in their tracks. This proactive shift toward real-time, collaborative defense is essential to restoring trust across the digital ecosystem.”

– Johan Gerber, Global Head of Security Solutions, Mastercard



How Mastercard CFR Works

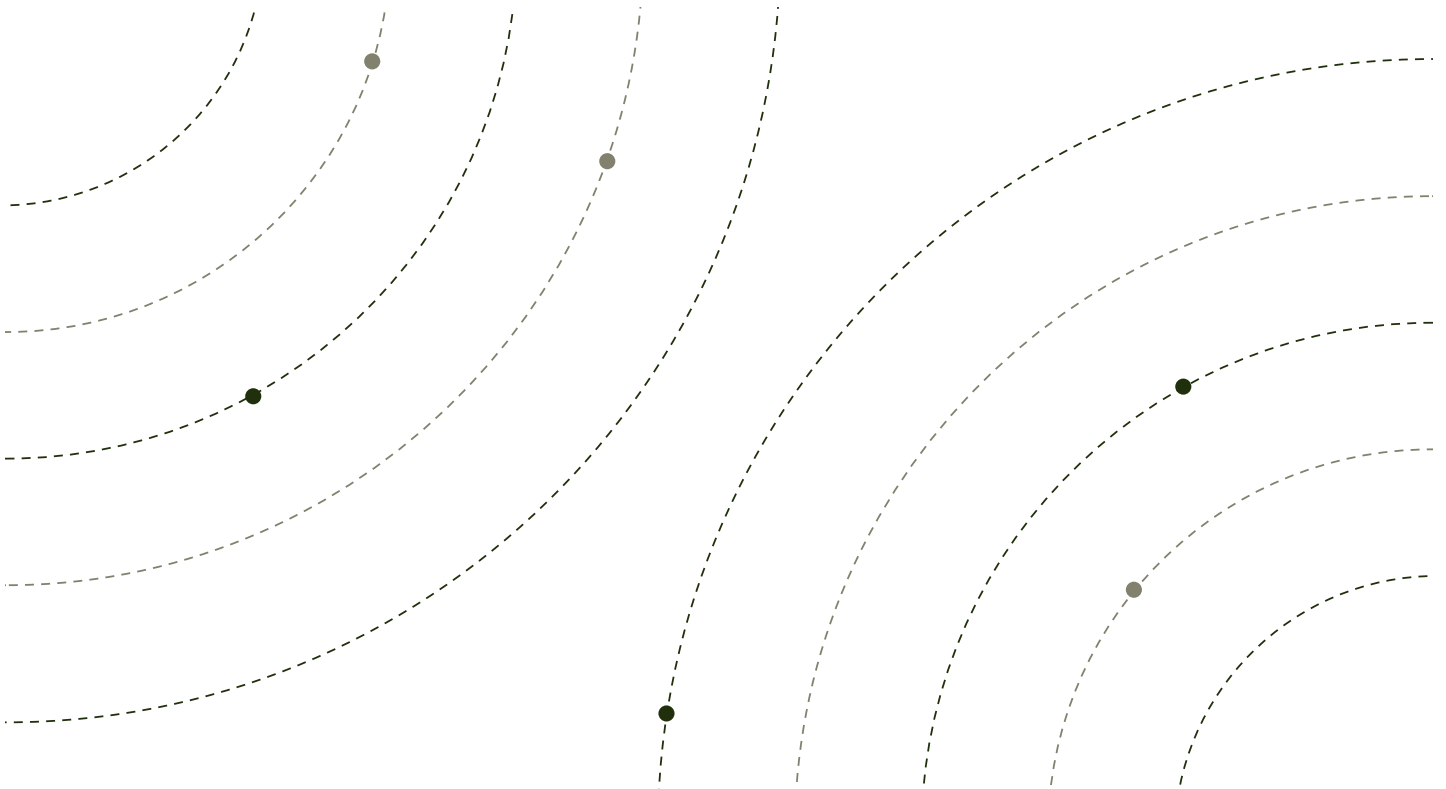


For each A2A transaction, CFR collects a plethora of attributes – account history, payment destination, transaction patterns, etc. Mastercard’s machine learning models (with Feedzai technology at its core) produce a risk score and additional data insights in milliseconds. These are delivered via API to:



- ➔ **Sender Bank:** The sender bank receives the score and data insights in milliseconds. If the score is high, the bank can take immediate action (pause the transfer, ask security questions, or flag the customer) before money leaves the account. If the risk score is low, it can be incorporated into existing models and rules to help reduce false positives. Today, 15 UK financial institutions use this system to help stop scams in real time.
- ➔ **Receiver's Bank:** Importantly, within seconds the receiver's bank gets the same risk score and data insights. If the transfer is destined for a known or suspected mule account, the bank can block the incoming funds or hold them for review. Early UK trials showed this approach enabled financial institutions to flag 60% more mule accounts,³ a trend that continues to hold as institutions scale adoption.

By scoring each transaction – incorporating signals from both the sending and receiving financial institutions, as well as the broader network – CFR delivers something no standalone ruleset can: a unified risk view just before the payment is executed. The result is genuine real-time performance!



³ <https://www.mastercard.com/global/en/news-and-trends/press/2024/september/mastercard-expands-first-of-its-kind-ai-technology-to-help-banks-protect-more-consumers-from-scams-in-real-time.html>



Real-World Impact (UK Case Study)

The UK provides a useful lens into how real-time scam-prevention capabilities are evolving across the industry. Since early 2023, several major financial institutions have incorporated CFR as part of broader efforts to strengthen fraud-mitigation strategies. During this period, national data showed that:



APP fraud cases **declined by ~20%** in 2024, compared to 2023 (from 232k to 185k).⁴ Since early 2023, the Mastercard solution has helped UK financial institutions to identify and stop authorized fraud transactions before the funds leave the victim's account.



Over **60% improvement** in mule account detection on inbound flows was observed. This means more fraud and scams were detected, helping UK banks to protect more consumers.⁵



15 financial institutions have now adopted CFR, covering about 90% of UK domestic A2A payments.

⁴ The UK Finance Annual Fraud Reports from 2024 and 2025 show a decline in case volumes, an improvement to which CFR has contributed alongside other influencing factors.

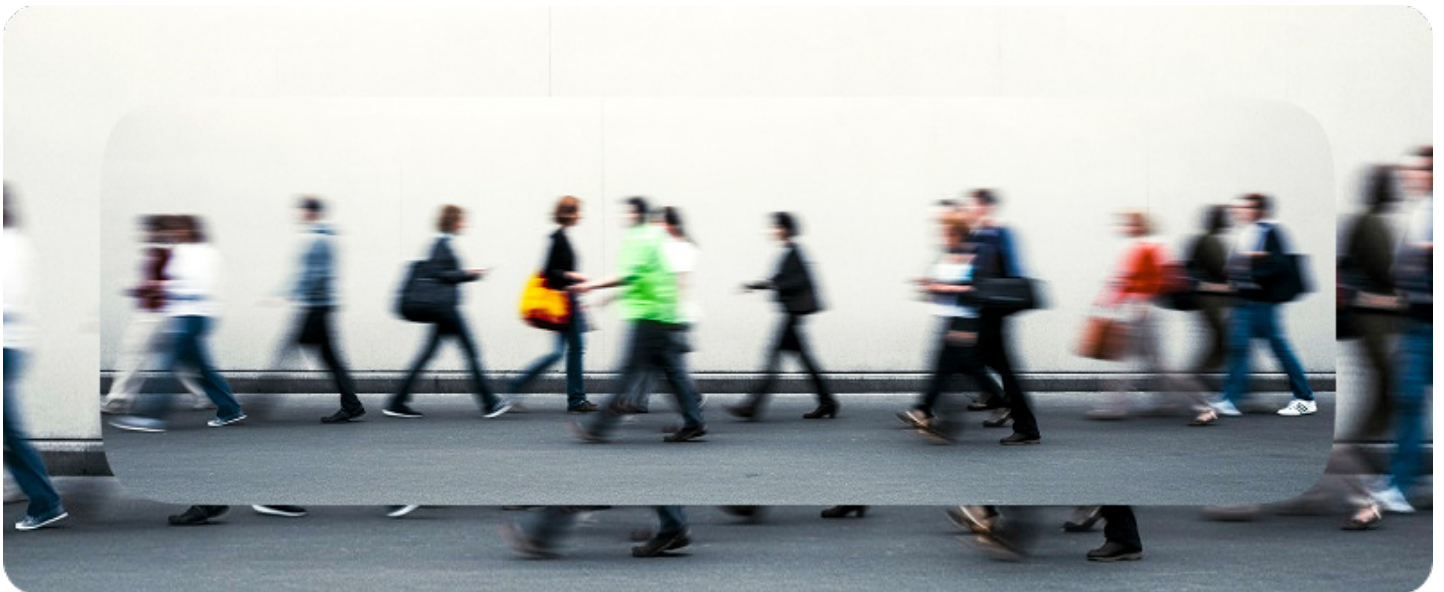
⁵ <https://www.mastercard.com/global/en/news-and-trends/press/2024/september/mastercard-expands-first-of-its-kind-ai-technology-to-help-banks-protect-more-consumers-from-scams-in-real-time.html>



These gains equate to substantial savings: even a 10% increase in incremental detection could prevent **tens of millions** in annual customer losses. As previously announced by Mastercard, Mastercard plans to extend CFR beyond the UK, with Feedzai providing the scalable engine.⁶

“Together with Feedzai’s global platform we will scale our first-of-its-kind scams solution to more markets, helping more financial institutions combat financial crime faster than before”

– Johan Gerber, Global Head of Security Solutions, Mastercard



⁶ <https://www.mastercard.com/mea/en/news-and-trends/press/2025/february/mastercard-and-feedzai-join-forces-to-protect-more-consumers-and-businesses-from-scams.html>



Strategic Benefits of the Feedzai-Mastercard Partnership

This partnership combines several differentiators:

AI-Native Infrastructure:

Feedzai's platform was designed from inception to operate at transaction speed. Models can be retrained and deployed into production quickly, enabling quick response to new scam activity. When confirmed outcomes flow back into the system, models continuously adapt, ensuring protection evolves as scam tactics change. All of this occurs without manual intervention.

A Shared Fraud Intelligence Layer Across the Network:

CFR operates as a unified intelligence layer that connects both sides of an A2A transfer across rails. This networked view transforms isolated signals into collective defense: emerging scam patterns identified in one institution or market instantly strengthen detection everywhere. By linking senders and recipients in real time, CFR exposes mule networks and coordinated attacks that siloed systems cannot see.

Real-Time & Scalable:

The solution scores transactions in milliseconds for the sending bank and an equally fast alert for the receiving bank. Feedzai's cloud-native architecture already handles billions of transactions per year. It has been proven to protect **\$8+ trillion** in payments for over a billion users worldwide, demonstrating the scale needed to protect global rails.



Call to Action

The era of payment fraud demands collective action. We urge SVP and C-suite leaders to:

- ➔ **Embrace Network Intelligence:** Sharing risk data doesn't dilute your security – it multiplies it across the entire payment ecosystem.
- ➔ **Augment Your Current Risk Strategies:** Incorporate shared early-warning signals and industry-wide fraud indicators to surface emergent threats.
- ➔ **Leverage Mastercard CFR:** Engage with Mastercard to pilot or integrate CFR in your real-time and P2P channels.
- ➔ **Reap the Benefits:** By adopting network-based fraud prevention, financial institutions can reduce losses and build trust while regulators see results. Early adopters will turn fraud defense from a cost center into a competitive advantage.

Mastercard and Feedzai have demonstrated that intelligence at scale works. The data is clear: AI-powered, network-wide prevention outperforms siloed defenses. The time to act is now! Don't let the next wave of real-time scams catch you unprepared.



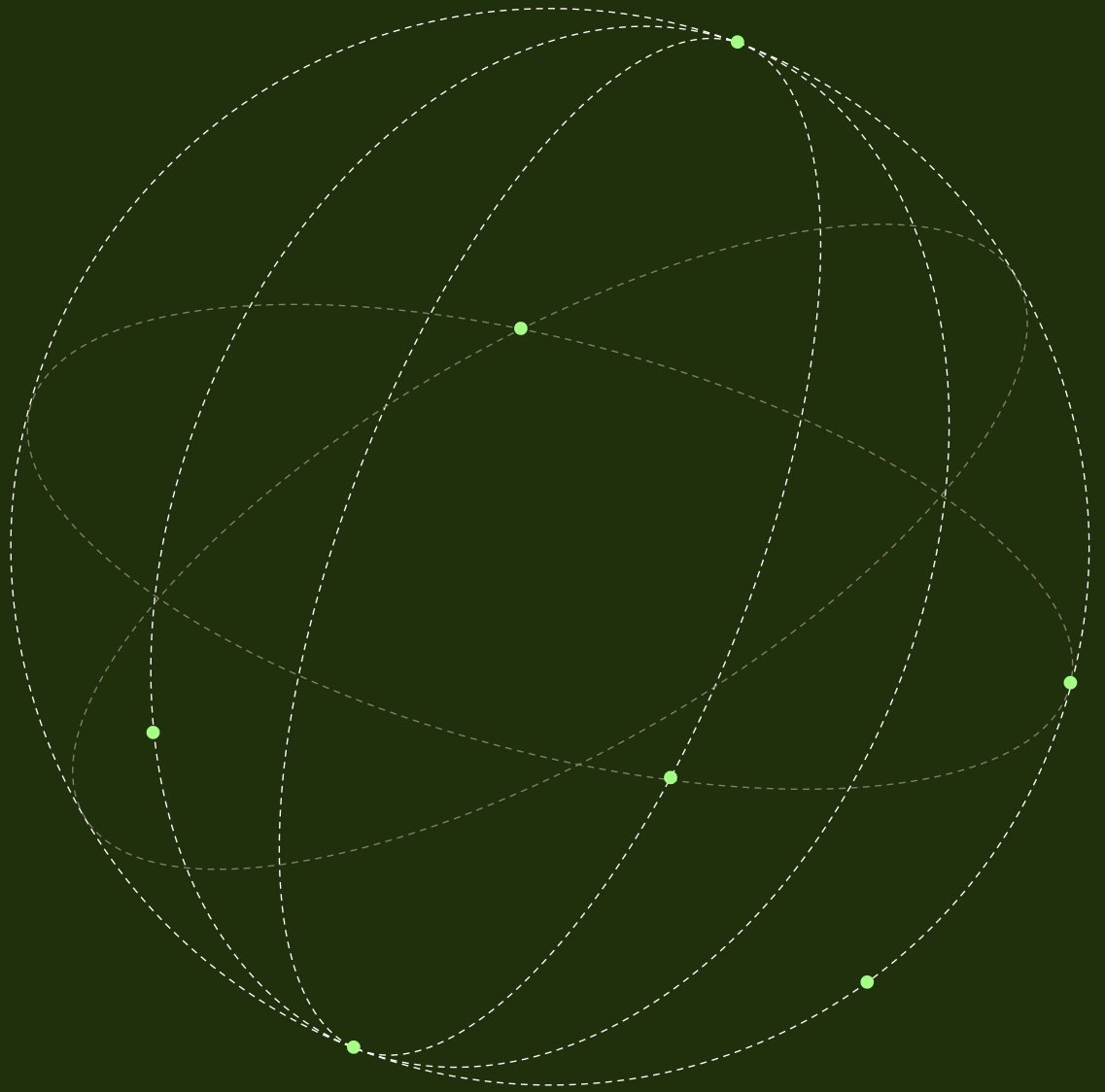
“Together with Mastercard, we’re redefining fraud prevention to help build a world of safer money. By combining AI-native, real-time intelligence with unmatched expertise and global reach, we’re strengthening trust across billions of transactions for millions of people and businesses.”

– Nuno Sebastião, Co-Founder and CEO, Feedzai

Contact Mastercard today to bring network intelligence into your fraud prevention arsenal.

Know more





Feedzai is the world's first end-to-end financial crime prevention platform, protecting people and payments with AI-native solutions that stop fraud and financial crime. Leading financial institutions trust Feedzai to manage critical risk and compliance processes, safeguarding trillions of dollars of transactions, while improving the customer experience and protecting the privacy of everyday users.

Recognized by



Celent.

Chartis

Identity

Orchestration

Fraud

Anti-Money Laundering

sales@feedzai.com

info@feedzai.com

feedzai.com