Targeting Fraud Today: A Real-Time, Integrated Approach

A Chartis/INETCO case study

Faced with complex fraud attacks and tech-savvy fraudsters, financial institutions struggle with slow, siloed and unwieldy systems. As highlighted by this case study at a Tier 2 bank, with real-time, AI-augmented fraud detection and prevention, firms can pinpoint fraud and strengthen their operations.

Context: the multidimensional challenges of modern fraud

Chartis has observed that the fraud landscape across payment ecosystems is undergoing a structural shift, driven by the convergence of AI-enabled attack capabilities, increasingly fragmented data environments and expanding exposure across payment infrastructure.

Fraudsters have long demonstrated technological sophistication, but the widespread availability of advanced AI tools has significantly accelerated the scale, speed and adaptability of attacks. AI is enabling more convincing social engineering, synthetic identities, automated fraud orchestration and increasingly complex transaction patterns that are harder to detect using traditional fraud controls.

At the same time, payment ecosystems have become more distributed and data-intensive. Financial institutions now manage vast volumes of structured and unstructured data across siloed systems, channels and jurisdictions, creating inconsistencies in visibility, control coverage and data quality. Fraudsters are increasingly exploiting these operational and architectural gaps – including blind spots between systems, delays in detection and fragmented monitoring approaches.

Chartis also sees a notable evolution in the focus of attacks: from targeting individual accounts and users toward exploiting the payment infrastructure itself. These infrastructure-level attacks often occur within trusted environments and leverage legitimate credentials, authorized workflows or accepted payment protocols, making malicious activity significantly harder to distinguish from genuine transactions. As a result, fraud detection is evolving beyond isolated transaction monitoring toward continuous, ecosystem-wide intelligence and behavioral analysis across the payment lifecycle.

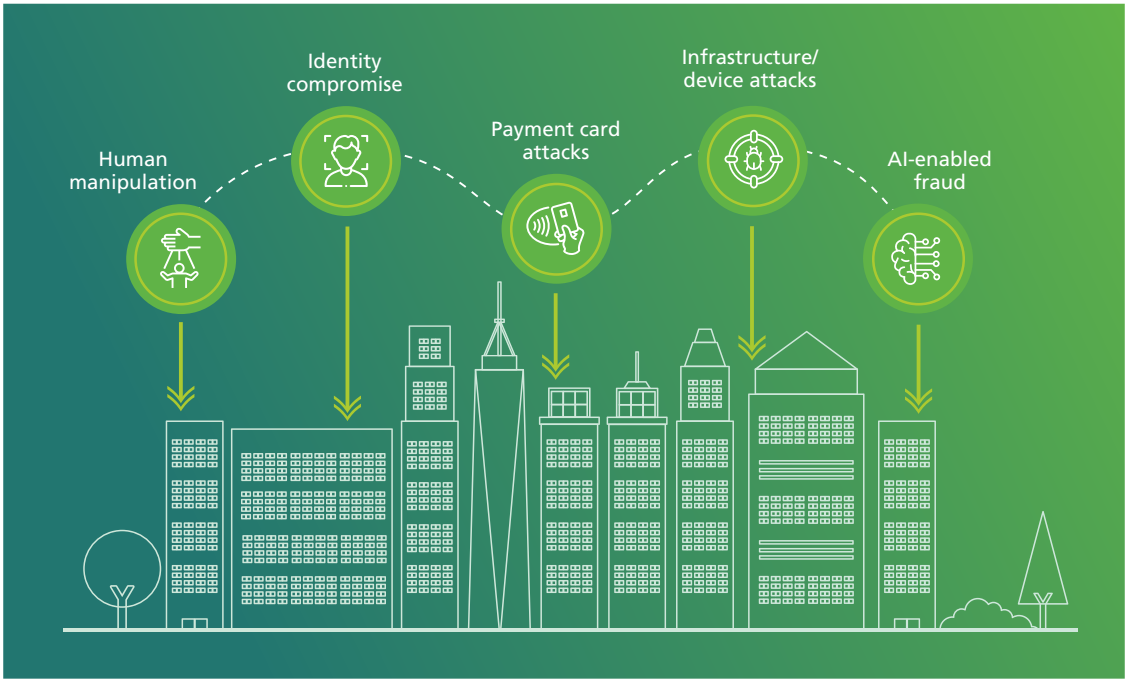
Increase in targeted attacks

Fraud has evolved from high-volume attacks to highly targeted, AI-driven strikes executed across multiple attack vectors, including:

- **Payment card attacks**. These include card-present/card-not-present fraud, card testing and rogue terminals.
- **Human manipulation**. Phishing, vishing, smishing, authorized push payment (APP)/scam frauds.
- **Identity compromise**. Identity theft, synthetic identities, account takeover, SIM swaps.
- **Infrastructure/device attacks**. ATM fraud, malware attacks, near-field communication (NFC) relay attacks, injection attacks.
- **Emerging AI-enabled fraud**. Deepfakes, money mule orchestration, botnet attacks.

Increasingly, these attacks do not occur in isolation – they are connected (see Figure 1). Using AI and sophisticated analytics, modern fraudsters craft unique profiles for each attack. By the time a traditional, rules-based system identifies a recognizable 'pattern', the fraudster has already changed their tactics, rendering static defences obsolete.

Figure 1: Fraud vectors – targeted and connected



Source: Chartis Research

Existing fraud detection and prevention systems – disjointed and reactive

For many financial institutions attempting to fight fraud, technical complexity remains the main barrier: in surveys carried out by Chartis, 42% of institutions identify integration challenges as their biggest obstacle. Many firms still rely on siloed detection systems that are reactive by design and often miss critical sub-second signals. In a digital payments ecosystem where transactions settle in milliseconds and are often irrevocable, detection capabilities that respond minutes and hours later to behavioral drift, suspicious account activity, device changes and network anomalies identify fraud only after losses have occurred.

This reactive approach creates failures on two fronts: evolving and zero-day fraud schemes pass through undetected, while legitimate customer transactions are unnecessarily impacted by broad, batch-driven controls that lack accuracy and precision. The result: eroded customer trust, direct revenue loss, increased operational strain and churn. Financial institutions can no longer treat security as a one-time 'check' at the front door – effective security now requires constant, orchestrated vigilance across the end-to-end transaction journey. While there have been significant advances in independent point solutions such as facial biometrics, strong authentication, Know Your Customer (KYC) and device intelligence, these tools often operate independently, generating isolated risk scores and different data elements rather than a unified view of transaction risk.

And from a data perspective, most application performance monitoring and logging solutions operate with a limited, component-specific perspective, capturing data elements that relate to specific solution components, such as web, application or database servers – which is not a Know Your Transaction (KYT) capability. Because events for each component are logged in isolation, financial institutions are unable to correlate and 'stitch' these events together in real time. While these solutions are essential for system resilience, they focus on collecting data related to availability or application performance, and lack the granular message-level transaction intelligence, which is vital for fraud detection.

Fragmentation and limited data visibility make orchestrating the real-time detection of fraudulent events within and across multiple channels a significant challenge. As a result, financial institutions are left struggling with a disjointed view of the risk landscape. Aware of the 'holistic view' challenge, more than 90% of financial institutions are pursuing data orchestration initiatives, according to Chartis' research.

Beating fraud in the modern era

Faced with evolving fraud, delayed detection and fragmented data visibility, financial institutions need a new set of capabilities: real-time, unified fraud prevention solutions that can act with speed, accuracy and precision. Chartis research suggests that to effectively detect and stop modern – and increasingly AI-driven – fraud attacks, financial institutions should have the following capabilities:

- **Granular, field-level data visibility for every end-to-end transaction, across all channels**: the ability to collect, correlate and analyze granular data elements related to the individual messages sent as part of a payment transaction journey. This KYT approach can enable financial institutions to detect and block fraud attacks with precision – before they complete.

- **Real-time decisioning**. Rules engines that can make decisions on granular data elements, resulting in accurate real-time alerts.

- **A combinatorial machine learning approach**. Multi-vector fraud cannot be treated with a single approach. A multi-faceted approach includes adaptive, entity-level machine learning models that continuously learn and analyze the unique behaviors of each individual account, user, device and terminal. These self-training models refine with every transaction and incorporate analysts' decisions back into model training to detect fraud in milliseconds, block it with precision and increase risk score accuracy.

- **Explainable AI**. Complex AI needs to be understandable. AI requires decisioning that provides clear reasoning for actions taken, to support trust, compliance and auditability.

- **Automated case management**. A workflow-driven investigation environment needs to unify the different fraud vectors into a single view that enables fraud analysts to review, correlate and drill into related transactions.

- **AI-assisted fraud investigation**. Agentic AI fraud agents that can help fraud analysts handle growing case workloads more effectively and efficiently by assisting in the triage of alerts, the prioritization of cases for immediate analyst attention, and the reduction of manual false positive reviews. AI agents can continuously improve via closed-loop analyst feedback and small language models that are specially trained.

- **Collaborative fraud intelligence**. This can enable financial institutions to detect and prevent fraud collectively on both a regional and a global scale.

The ideal outcome is highly targeted, real-time fraud detection and prevention at scale – enabling financial institutions to stop fraudulent in-flight transactions before completion, without resorting to blocking legitimate customers or batch-level processing after the fact.

Case study

INETCO at a Tier 2 bank: real-time, targeted measures

The client: Tier 2 bank, based in South Africa.

The problem: The bank was using rules-based systems that were fragmented and reactive, with limited real-time decisioning capability and significant visibility gaps across channels. This led to issues with detection lag, high numbers of false positives, fragmented fraud visibility and poor adaptability. The bank required a fundamentally different approach: a unified, low-latency fraud decisioning layer that could operate at scale, in real time, without disrupting the legitimate customer transactions the bank worked so hard to enable.

The INETCO BullzAI solution: The solution focused on alleviating complex fraud with real-time, individualized fraud detection and prevention. INETCO BullzAI introduced a real-time fraud decisioning layer within the bank's environment that decodes every end-to-end transaction at the protocol level, enriches it with device, behavioral and contextual intelligence, and evaluates risk within milliseconds.

- Detection now occurs after self-training AI models focus on transactions at the level of individual entities' behavior, ensuring that each account, card, device and terminal is assessed.
- Risk scores and actions are available in real time, consolidating activity for each individual account, card, device and terminal across multiple channels (including ATM, point of sale [POS], mobile, internet and real-time payment rails). Scores are updated continuously after every transaction without requiring intervention from external vendors or data scientists.
- High-risk transactions are blocked in-flight before authorization, ensuring that legitimate customer transactions can continue and fraud is prevented before losses occur.
- Fragmented, reactive workflows are being replaced with more efficient, effective AI-assisted triage, explainable AI inferencing and closed-loop learning driven by analyst feedback.

INETCO BullzAI's capabilities were put to the test during a national PayShap instant payments surge event, during which fraudulent activity spiked dramatically. Within minutes, INETCO BullzAI's machine learning models identified the suspicious patterns and the transaction firewall blocked the high-risk transactions before they reached the authorization host, while legitimate customers continued transacting without interruption. This was not just a technology validation – it confirmed that the entire operating model behind the platform was sound. The bank has shifted from reactive, fragmented controls to real-time, end-to-end fraud prevention at the transaction level across all channels.

> *'We obsess about delivering the best solutions for our customers and ensure that we focus on their security. This additional layer of fraud prevention allows us to match our digital growth with world-class protection. With INETCO BullzAI, we've shifted from a reactive model to a proactive AI-driven strategy that enables us to detect and block increasingly sophisticated and unknown fraud patterns in real-time, allowing us to meet compliance requirements, prevent fraud before it causes harm and deliver the safest possible banking experience.'*
>
> **Group Chief Operating Officer**

Conclusion

The transformation and modernization of payment services to make them closer to real-time has shortened the fraud detection window. This has resulted in the reduced effectiveness of batch and rules-based controls.

To beat fraud, financial institutions need real-time KYT intelligence to understand user, card, device and terminal activity, and to analyze what constitutes normal or anomalous behavior. By focusing on behavior, fraud teams can detect subtle deviations from individualized historical patterns that static, rules-based systems with a limited field of view can miss.

Pinpointing anomalies and intermediating transactions at the individual message level allows institutions to improve the accuracy and explainability of detection controls while reducing unnecessary friction for legitimate customers.

Many merchants and financial service providers face rampant fraud executed by botnets that produce thousands of false positives. This challenge is exacerbated by fraudsters' use of AI-powered automation tools. As highlighted by this case study, INETCO BullzAI leverages individualized machine learning models, a patented transaction firewall and AI-assisted investigation to adapt to new and evolving threats in real time and more accurately detect and block fraud, reducing noise and improving fraud operations mandates.

Ultimately, this ability to surgically throttle and block fraudulent transactions automatically, combined with AI-assisted investigation, frees up fraud teams, enabling them to focus their efforts on the highest-risk events rather than sifting through noise for signals.

About INETCO

Named a Category Leader in Chartis' 2026 Enterprise and Payment Fraud RiskTech Quadrants.

INETCO's mission is straightforward, yet urgent: deliver the payment security and reliability that all people deserve – every moment, every day. Headquartered in Canada, the company helps financial institutions, retailers, payment processors and FinTechs worldwide detect and prevent payment fraud and AI-driven cyber-attacks in real time – enabling organizations to outsmart fraudsters, stay compliant and keep customers safe. With deployments in more than 30 countries, INETCO monitors over 100 billion payment transactions annually.

Built on decades of payment expertise and trust, the patented INETCO BullzAI platform is redefining payment security by:

- Detecting zero-day attacks, multi-vector fraud and evolving threat patterns within milliseconds across all banking channels, including ATM, POS, mobile, internet and real-time payment rails.
- Blocking fraudulent transactions before authorization or financial loss occurs, without disrupting legitimate customer interactions.
- Delivering deeper behavioral insights for every customer, device and terminal through granular transaction intelligence, adaptive machine learning models and explainable AI.
- Increasing the efficiency and effectiveness of fraud case management with agentic AI capabilities and proprietary small language models.

As payment fraud becomes increasingly sophisticated, INETCO continues to advance new standards of innovation for payment protection globally. The company is proud to empower millions of unbanked and underbanked people around the world by making real-time fraud prevention technology accessible in emerging markets such as Latin America, the Middle East and Africa – and enabling safe, inclusive and trusted participation in the digital economy. INETCO was named a Category Leader in Chartis Research's 2026 Enterprise and Payment Fraud RiskTech Quadrants.