



A WHITEPAPER

Building an Effective Payment Fraud Detection Framework: 8 “Must-Have” Components

CONTENTS

The Current state of digital payments	3
The evolution of payment fraud	4
Establishing a payment fraud management framework that works.....	6
Key components of top payment fraud detection and prevention software	8
Unlimited access to real-time payment transaction data.....	9
Real-time event monitoring	10
Link analysis and end-to-end transaction profiling	11
Rules based policy and alerts engine.....	13
Supervised and unsupervised machine learning	14
Behavioral analysis	16
Case management and workflows.....	17
Open APIs and fraud orchestration	18
How INETCO Insight leads the way in payment fraud detection	19
Summary	20
Endnotes	20

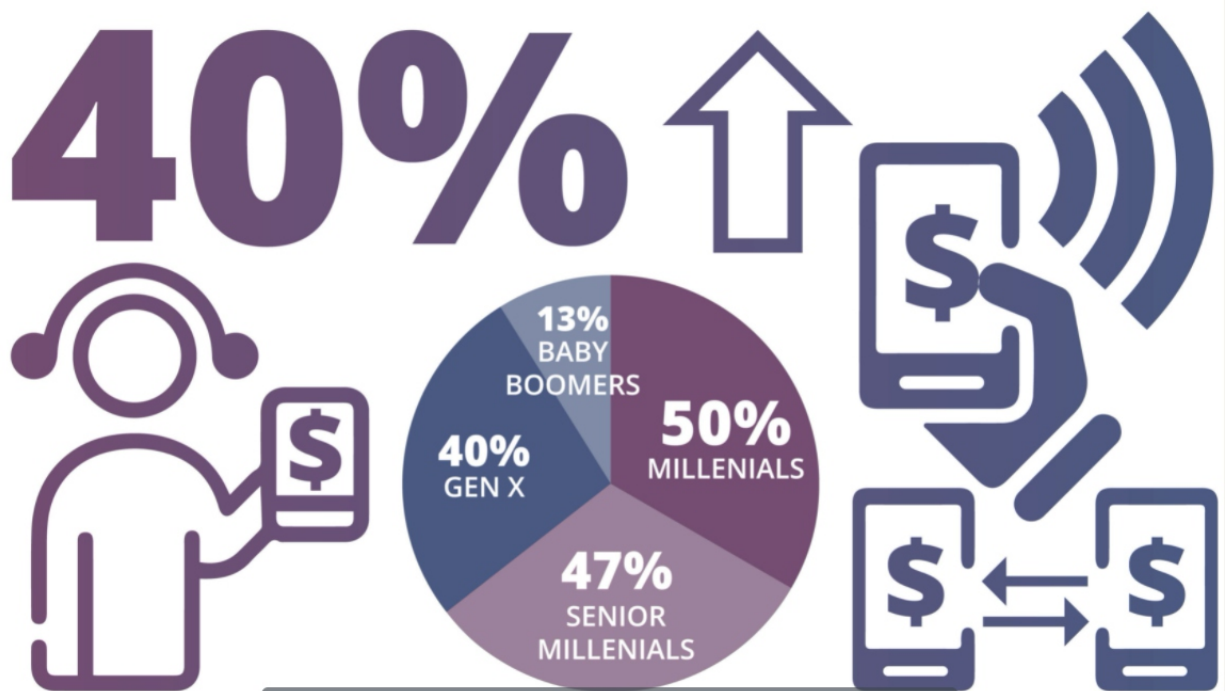
The current state of digital payments

COVID-19 has accelerated the digitization of payments all over the world, setting the stage for the “next normal”. Credit and debit cards are continuing to gain major momentum in markets that have been traditionally cash-dominated, especially in the Asia Pacific and Latin American markets. Globally, we continue to see the rising adoption of contactless and card not present payment options. During the first quarter of 2020, MasterCard reported a **40% jump in contactless payments** – including tap-to-pay and mobile pay – mainly driven by the worsening of the global pandemic.¹

The use of convenient, alternative payment rails such as instant payments, social commerce, online and mobile continue to be on the rise. According to Aite Group's researchⁱⁱ, digital-first will be the new norm in banking. Fifty percent of young millennials, 47% of senior millennials, 40% of Gen Xers, and 13% of baby boomers pay at a store or online, send money, or receive money using Venmo, Facebook, Google Wallet, PayPal, or Square Cash at least once a week.

In addition to increased tech and smartphone savviness, there is growing synergy between governments, banks, fintechs, and payment service providers that are working together to deliver safe, reliable payment services.

The pandemic has compressed a half-decade worth of change into less than one year—and this is happening in areas that are typically slow to evolve, such as customer behaviour, economic models, and payment operating models. The consensus is that digital payments are not disappearing, and will only increase in popularity over the years to come. And with this ongoing acceleration towards digital, comes a barrage of criminals, ready to exploit every point of weakness throughout these new payment journeys.





With the increase in digital payments has come an exponential increase in payment fraud attacks.

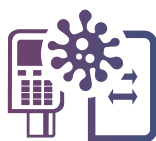
The evolution of payment fraud

The increase in digital payments has been accompanied by an exponential increase in payment fraud attacks. Fraudsters see the accelerated digital transformation as an opportunity to exploit weak links in the end-to-end payment transaction chain. They are continuously inventing new mechanisms to perpetrate fraud, meaning you must be ready to increase the resiliency of your payment systems to make certain your security is not outpaced by your digital innovation and growth. This involves thinking about fraud mitigation and security across every transaction type – including card present, card not present, contactless, real-time payments, and third-party payment services. Ultimately, you will need to deliver the level of trust, security, and service consumers are relying on - across all payment rails and banking channels.

Guaranteeing the safety of every payment transaction involves protecting a growing attack surface and staying ahead of the volume and variety of payment fraud and cybersecurity attacks that have become prevalent with COVID-19. Here are a few types of threat vectors that have been spotted more often since the outbreak of the pandemic earlier this year:



Card-present (CP) and card-not-present (CNP) fraud – CP and CNP fraud involve fraudsters using stolen account credentials, personal identification numbers (PINs), or card information to make purchases or deposits you did not authorize. This includes purchases at a place of business, or transactions online. CP and CNP fraud often happen when credit, or debit card numbers are given out to a fraudster by mistake, when cards are lost, or stolen, when mail is diverted, or when a malicious actor copies the cards, PINs, or card numbers. Credit card skimming and PIN capturing devices are used to capture data from the magnetic stripe on the back of a card and are most commonly inserted by fraudsters at ATMs, gas pumps, or other POS devices.



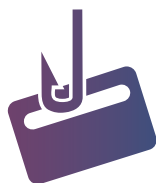
Man-in-the-middle attacks – A man-in-the-middle attack exploits the real-time processing of transactions, conversations, or transfer of other data. It is a type of eavesdropping attack that occurs when a malicious actor inserts himself (via malware) as a relay/proxy into a communication session between people or systems. These attacks often involve criminals breaching a bank, or payment card processor to manipulate fraud detection controls as well as alter customer accounts. This type of fraud is commonly the perpetrator of ATM cash-outs, jackpotting attacks, and has also been used to intercept customer emails containing bank details. In the latter case, the fraudster changes the sort code and account numbers in an attempt to redirect funds to their own account.



Automated botnet attacks – An internet bot is commonly used by hackers to perform a “distributed guessing attack”. Bots are used to instigate malicious activities such as credentials leaks, unauthorized access data theft, and Distributed Denial-of-Service (DDoS) attacks.



Account takeover fraud – An account takeover attack is a form of identity theft. A malicious actor tries to gain access to a user's account credentials. This is typically done using automated bots to access banking account details, perform credential stuffing, carding, ticketing, or brute force attacks on scale, or break into an e-commerce site. If successful, an account takeover leads to fraudulent transactions and unauthorized shopping from the victim's compromised account.



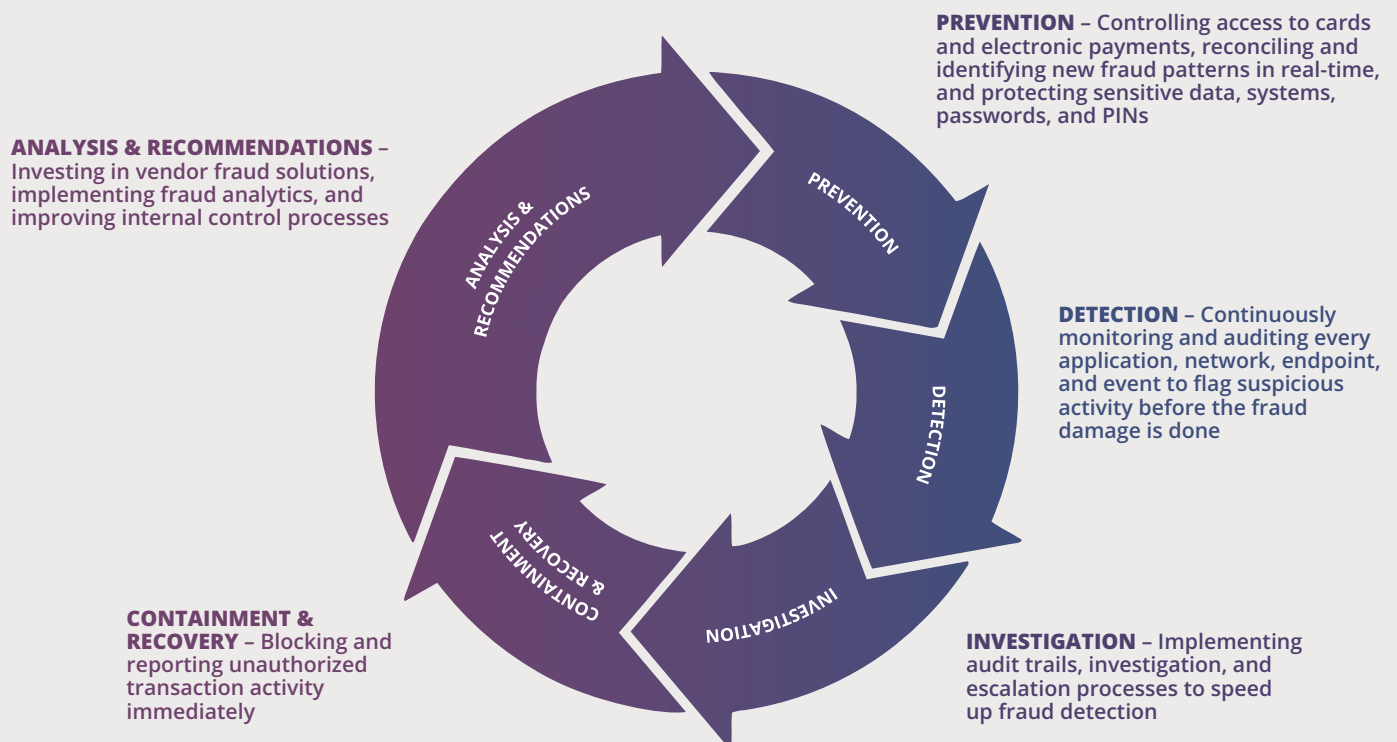
Phishing scams – Phishing attacks involve sending fraudulent communications that appear to come from a reputable source. Fraudsters hope to steal sensitive data, such as usernames, passwords, and credit card details, by disguising oneself as a trustworthy entity. Examples of different types of phishing attacks include emails, spear phishing, link manipulation, fake websites, CEO fraud, session hijacking, malware, and content injection. Phishing scams are also used to install malware on the victim's machine.

Establishing a payment fraud management framework that works

Digital payment fraud will not disappear, but there are things you can do to minimize the impact. A good place to start is building out a fraud-fighting strategy that minimizes financial loss, reputational harm, and unnecessary payment transaction declines.

In response to customer behavioral shifts and the rise of fraud through digital payment channels, many issuers, acquirers, and merchants are overcompensating by either dialing up their existing fraud risk scoring criteria or not adapting existing risk scoring models fast enough. Either way, the result is a greater number of payment transactions flagged as fraudulent. The problem is, that many of the transactions they are declining are genuine. In addition to increased customer friction, the Aite Groupⁱⁱⁱ estimates that in the United States, **\$443 billion USD in revenue** will be lost due to false declines in 2021—nearly 70x more than the projected losses from card-not-present fraud itself (\$4.6 billion USD by 2021).

To approve more good transactions, stop more fraud, and make decisions faster, you need a multi-channel payment fraud management framework designed to keep up with fast changing customer habits and evolving fraudster sophistication. It will be important to adopt a framework that covers off:



Effective risk and cybersecurity management requires your payment fraud detection capabilities to extend across the entire customer payment transaction journey. Armed with the right payment fraud detection and prevention software, you can defend against a variety of automated and human attack vectors, and enhance the security of every end-to-end payment.

Key components of top payment fraud detection and prevention software

Detecting and preventing payment fraud requires an in-depth assessment at every step along the customer payment journey. This end-to-end journey typically starts with a login, a card tap, a wallet swipe, or a card insertion. The ability to continuously see across every initiated transaction — from the customer endpoint to the host or third party service authorization, and back for completion is a methodology that promotes the elimination of siloes by orchestrating fraud management decisions from a single platform. It requires both continuous discovery, monitoring, assessment, and risk prioritization to get full visibility and context of assets and risk, including prioritization of vulnerabilities, as well as both adaptive attack and access protection.

To successfully detect and prevent payment fraud in real-time requires an advanced set of components, and each one must operate in concert with the others. Conducting a continuous assessment of risk and trust means you cannot architect in silos – your approach should be an integrated, adaptive system.



KEY COMPONENTS OF TOP PAYMENT FRAUD DETECTION AND PREVENTION SOFTWARE TO CONSIDER INCLUDE:

Component	Benefits for FIs and merchants
 <p>1. Full access to real-time payment transaction data (across all payment rails and channels)</p>	<ul style="list-style-type: none"> Assess the risk of every payment transaction in milliseconds – regardless of the customer endpoint or payment rail. Provides a single source of data for decision analysis allows to make faster decisions.
 <p>2. Real-time, multi-channel event monitoring</p>	<ul style="list-style-type: none"> More easily identify weak points where fraudsters infiltrate or third party issues. Respond faster to fraud alerts, meaning lower fraud losses.
 <p>3. Link analysis and end-to-end transaction profiling</p>	<ul style="list-style-type: none"> Detect man-in-the-middle attacks where malware is placed on a transaction switch to approve transactions without them reaching the authorization host.
 <p>4. Rules-based policy and alerts engine to identify fraud</p>	<ul style="list-style-type: none"> Set alerts for the entire payment network, not just the backend authorization host to get a more comprehensive ability to detect and prevent fraud attacks.
 <p>5. Supervised and unsupervised machine learning anomaly detection</p>	<ul style="list-style-type: none"> Reduce false positives through the automatic creation of ML models for each customer and card. Generate real-time risk scores that can be leveraged to approve, decline, or require a step-up for each payment transaction. Provide fraud analysts with all the data they need to understand why an alert was triggered in a single UI, eliminating guesswork and improving productivity.
 <p>6. Behavioral analysis</p>	<ul style="list-style-type: none"> Detect new fraud schemes and attacks that are not yet exposed. Greatly speed up fraud detection and response times (combined with rules-based alerts and machine learning).
 <p>7. Case management and automated workflows</p>	<ul style="list-style-type: none"> Speed up triage and close payment fraud cases more efficiently.
 <p>8. Open APIs and fraud orchestration</p>	<ul style="list-style-type: none"> Benefit from the capabilities of multiple fraud vendors while keeping operational costs under control Increase agility in the face of evolving threats.



1. Full access to real-time payment transaction data (across all payment rails and channels)

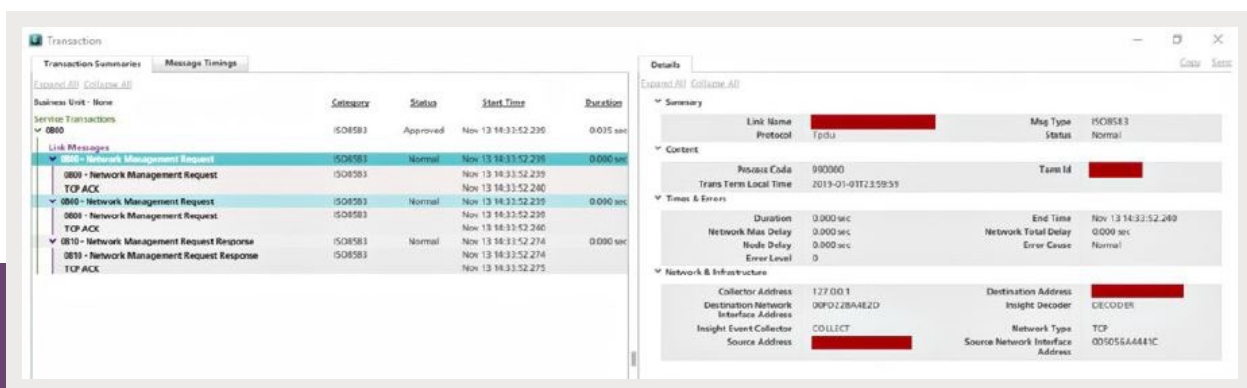
Your payment security will only be as good and fast as your data – and according to Julie Conroy³, research director of Aite Group's Fraud and AML practice, the number one pain point is harnessing internal data effectively: "Harnessing their data so that insights can surface represents a significant challenge for many firms, however; if not done right, the old adage 'garbage in, garbage out' is too true."

Performing continuous, data-driven decisions related to fraud risk requires a solution that collects and correlates data across every link of the end-to-end payment transaction journey – regardless of application, language, payment rail, or channel. Multi-link data collection and correlation is necessary to break down data siloes across customer endpoints, applications, payment rails, banking channels, and network transition points because these are the weak points where fraudsters infiltrate.

To avoid detection lag times and access enhanced data elements for analysis, all payment message fields, metadata, response-request timing, and network communications information should be decoded in real-time.

It is important to make sure that no valuable contextual information (e.g., terminal ID, EMV data element, IP address) is stripped at the terminal handler or payment switch level.

INETCO'S CLIENT SUCCESS: Real-time transaction profiles provide one of our customers, [Evertec](#), one of the largest merchant acquirers in Latin America, with a one-stop view into the network communications data and application payload messages contained within every link of an end-to-end transaction. Their team in Costa Rica can identify fraud before it happens.



Transaction Summary				
Business Unit - Name	Context	Status	Start Time	Duration
Service Transactions	ISO8583	Approved	Nov 13 14:33:52.235	0.035 sec
0000				
Link Messages				
0000 - Network Management Request	ISO8583	Normal	Nov 13 14:33:52.235	0.000 sec
TCP ACK			Nov 13 14:33:52.240	
0000 - Network Management Request	ISO8583	Normal	Nov 13 14:33:52.235	0.000 sec
TCP ACK			Nov 13 14:33:52.240	
0000 - Network Management Request Response	ISO8583	Normal	Nov 13 14:33:52.274	0.000 sec
TCP ACK			Nov 13 14:33:52.275	

Details			
Link Name	Protocol	Msg Type	Status
Summary	ISO8583	Normal	
Process Code	000000	Trans Term Local Time	2019-01-01T13:59:53
Duration	0.000 sec	End Time	Nov 13 14:33:52.240
Network Max Delay	0.000 sec	Network Total Delay	0.000 sec
Route Delay	0.000 sec	Error Cause	Normal
Error Level	0		
Collector Address	127.0.0.1	Destination Address	127.0.0.1
Destination Network Interface Address	00FD12B4E2D	Insight Decoder	DECODER
Insight Event Collector	COLLECT	Network Type	TCP
Source Address		Source Network Interface Address	005055A4441C

Benefits for FIs and Merchants

- Assess the risk of every payment transaction in milliseconds – regardless of the customer endpoint or payment rail.
- Single source of data for decision analysis allows to make faster decisions
- Easier to identify weak points where fraudsters infiltrate or third party issues
- Faster response to fraud alerts means lower fraud losses



2. Real-time, multi-channel event monitoring

While your payment fraud detection strategy should include multiple protection techniques, centralized real-time event monitoring is a must have when it comes to taking proactive and reactive action against payment fraud attacks – across all channels and rails. This involves tracing a payment transaction path through an entire enterprise infrastructure, and spotting suspicious transaction activity before customers do - without having to constantly observe or interrogate the system after the damage is done.

Real-time event monitoring helps you to automatically screen each link of an “in-flow” payment transaction, as it traverses across multiple customers' endpoints, technologies, and network infrastructures – making it easy to assess where missing transaction links, transaction path deviations, or suspicious transaction activity is occurring in milliseconds. This includes continuous visibility and assessment into customer usage, payment systems activity, application payload, and network.

INETCO'S CLIENT SUCCESS: [See how Moneris Solutions uses INETCO Insight transaction monitoring to monitor payment applications in over 350,000 merchant locations.](#)^{vi}

Benefits for FIs and Merchants

- Assess the risk of every payment transaction in milliseconds – regardless of the customer endpoint or payment rail
- Single source of data for decision analysis allows to make faster decisions
- Easier to identify weak points where fraudsters infiltrate or third party issues
- Faster response to fraud alerts means lower fraud losses





3. Link analysis and end-to-end transaction profiling

Transaction link analysis involves matching a user request to all the various back-end calls and services required to execute it. When it comes to malware detection and exposing risky transition points on the end-to-end payment transaction path, you will not be covered unless you establish holistic visibility into how in-flight transactions traverse across multiple nodes and networks.

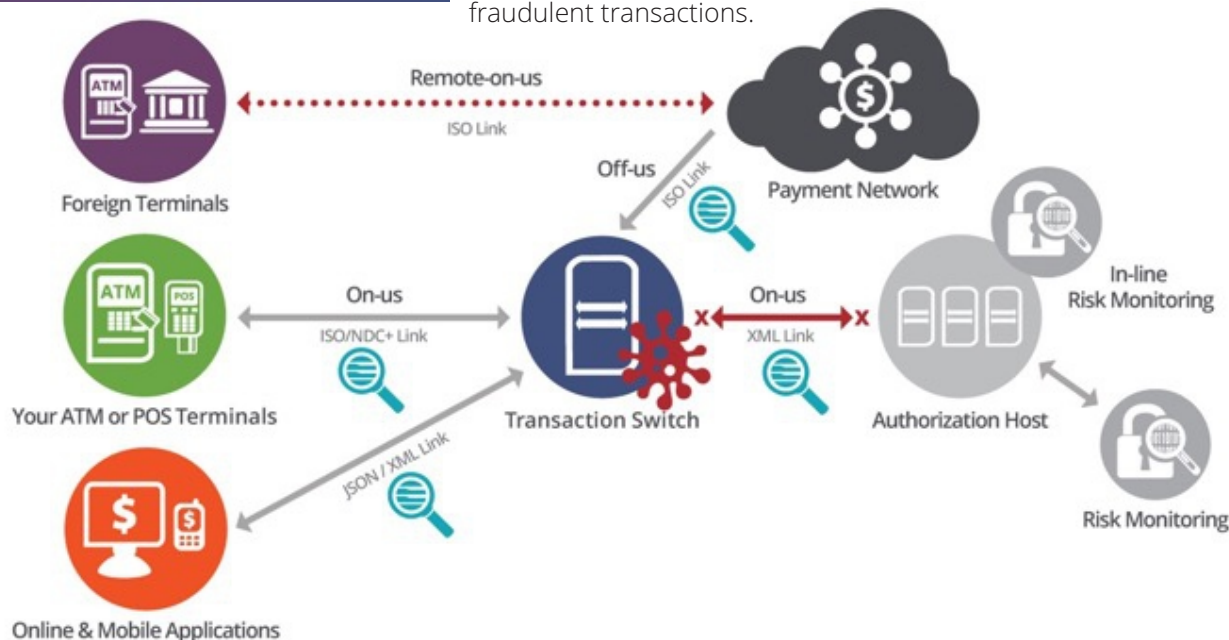
Using full transaction profiling, it is possible to reconstruct and establish a one-stop view into multi-protocol transactions – making it easy to see connections in your data that are strong indicators of fraud. Viewing the end-to-end transaction path and all the underlying network communications links and application payload details provides an efficient way to navigate through thousands of card present and card-not-present payment transactions so that you can speed up fraud detection and investigation.

Benefits for FIs and Merchants

Detect man-in-the-middle attacks where malware is placed on a transaction switch to approve transactions without them reaching the authorization host

Fraud Scenario: Man-in-the-middle attacks for ATM cash-outs.

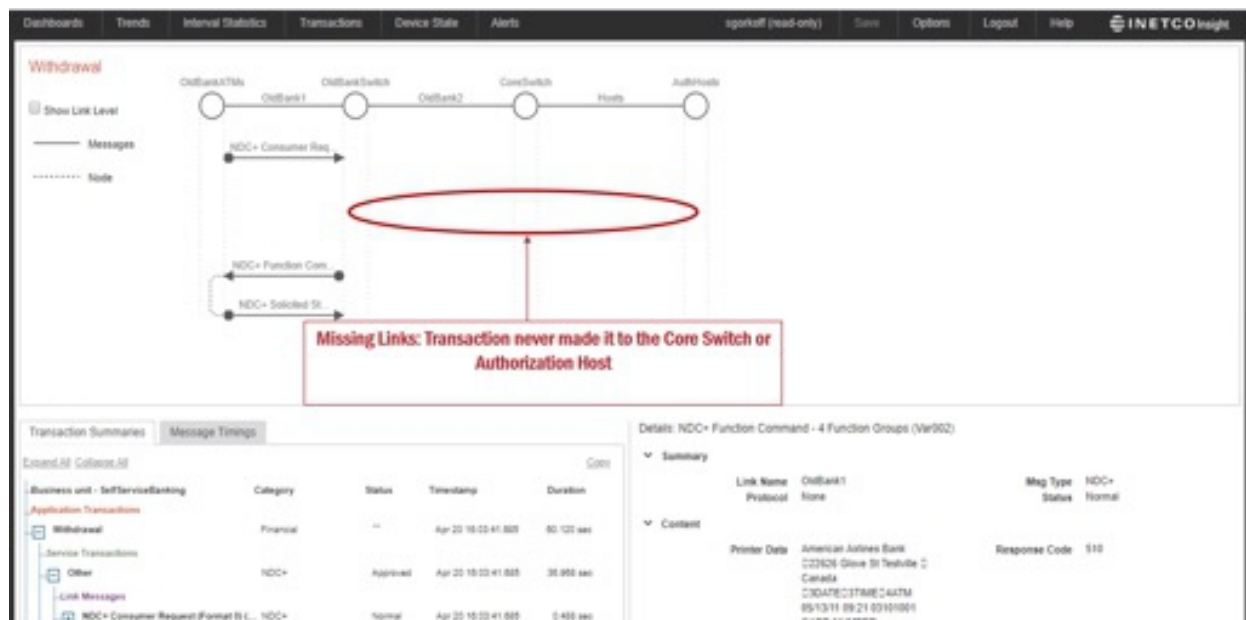
Malware is placed on a transaction switch, card information is then used to create cloned cards and distributed to money mules. Successive attacks are then launched from a large number of ATMs. Once the switch is compromised and the malware is activated, the transaction switch goes into a stand-in mode and starts to approve the fraudulent transactions.



Standard fraud detection solutions: As transactions never go to the back-end to be authorized, the limits on accounts are not enforced and fraud detection systems are blindsided. With fraud systems blind, an unlimited amount of attacks and withdrawals can happen without ever being detected or stopped. Millions of dollars get stolen.

INETCO Insight fraud detection:

INETCO Insight captures full transaction details for every end-to-end transaction in the customer's network in real-time. As INETCO Insight correlates every link in the end-to-end transaction, it can detect if links that should be present in a transaction are missing.



For this case, INETCO Insight triggers an alert if the system detects that there are missing transaction links (back-end transactions). Missing communication links for an approved transaction can indicate that malware, which bypasses the Authorization Host, has been installed on a transaction switch. The malware is approves fraudulent transactions or ATM withdrawals.

INETCO'S CLIENT SUCCESS: In late 2016, one of the largest financial institutions in Africa found themselves the target of a sophisticated, highly coordinated ATM fraud attack. 100 people had used forged credit cards to withdraw \$19M from 1400 ATMs in one city in under 3 hours. [See how we helped this financial institution to improve early warning fraud detection and avoid such cases.](#)^{vii}





4. Rules-based policy and alerts engine for fraud identification

Having the ability to create, test, and maintain rules is essential to choosing the right payment fraud management solution for your business. A configurable, rules-based alert engine applies a specific collection of policies and criteria to payment transactions in real-time. These rules play an important role in speedy bot detection, account takeovers, and the identification of suspicious transaction activity patterns. Rules can be created based on specific message fields (e.g. payment transaction dollar amount, volume or velocity), thresholds, sanctions, and watch list screenings.

Example alerts include:

- Transaction risk score for card or customer ID exceeds threshold
- Too many device fingerprints and IP geolocation changes
- Cash withdrawal observed on an ISO link with no matching database transaction (man-in-the-middle attack)
- Repeat card usage or customer ID by device, distance, or store
- Repeat account log-in attempts
- Repeat terminal usage (cash-out attack)
- Distance based card usage or device log-ins
- High ticket purchases or rapid succession of transactions
- High withdrawal velocity in a short amount of time
- Unexpected EMV fallbacks, high reversals and stand-in modes
- Status and response code errors
- Card being used is black listed or a mobile device is being used in a country in a negative country list

Benefits for FIs and Merchants

Set alerts for the entire payment network, not just the backend authorization host which results in a more comprehensive ability to detect and prevent fraud attacks.

Alert management capabilities allow for the quick review of flagged or blocked transactions. Transaction details related to devices, accounts, cards, data network links, third party connections, and payment applications can be immediately viewed and assessed for risk. Alerts should be easily forwarded into existing fraud orchestration, case management, support ticketing, and dispatch systems of choice.

INETCO'S CLIENT SUCCESS: [See how BECU enhances member experience with rules-based alerts and machine learning capabilities to detect ATM cash-outs and other transaction-level payment fraud attacks in milliseconds.](#)^{viii}





5. Supervised and unsupervised machine learning

Supervised and unsupervised machine learning form the core of advanced fraud management offerings such as risk scoring, new fraud pattern detection, and predictive modelling. These are adaptive models - built upon several transaction attributes - that learn from customer behaviors and become more accurate over time. Machine learning models are often layered with rules-based alerts and behavioral analytics to immediately pick up on anomalous behavior as machine learning becomes more accurate over time.

In supervised machine learning, data from valid and fraudulent transactions are used to recognize fraud based on historically confirmed fraud cases and requires a human to be involved. In unsupervised machine learning, the models learn dynamically, surveying transactions in order to identify new suspicious patterns. These models are ideally built out to look at anomalies on a per-customer or -device basis, and enable the detection of previously unknown, emerging fraud.

Over the past year, self-learning algorithms have become a lot easier to configure, and are often built on flexible algorithms such as Isolation Forest and Gradient Boosting. Newer models support continuous data feeds and incorporate seasonality, individual real-time transaction events, and in-depth transaction attributes to increase real-time risk scoring precision. Real-time risk scoring and configurable models that understand evolving transaction patterns in real-time should be considered as a requirement. Pre-COVID models that base the assigned risk value on historical data that is not up to date may no longer be valid – resulting in an increase of false positives.

Fraud Scenario: Five transactions of greater than \$1000 are made on the same PAN (card) in a 60-minute period. The fraudster is using a stolen card to charge a number of high-value transactions in a short period of time.

Benefits for FIs and Merchants

- Reduce false positives through the automatic creation of ML models for each customer and card.
- Generate real-time risk scores that can be leveraged to approve, decline, or require a step-up for each payment transaction.
- Provide fraud analysts with all the data they need to understand why an alert was triggered in a single UI, eliminating guesswork and improving productivity.

Solution: Automatically create a unique ML model for each card and trigger an alert based on a risk score that is unique for every PAN, instead of an absolute value. The purchase pattern of each customer is unique, so the model will be better able to spot real fraud instead of flagging a genuine transaction.





6. Behavioral analysis

According to a global study, by the end of 2024, 75% of enterprises will shift from piloting to operationalizing AI, driving a 5X increase in streaming data and analytics infrastructures. Data visualization, graphical trends, and analytics combined with artificial intelligence technologies will be paramount in the effort to predict, prepare and respond in a proactive and accelerated manner.

Dynamic behavioral analytics, combined with rules-based alerts and machine learning, can greatly speed up fraud detection and response times. Information is tracked in profiles that represent the behaviors of each customer, account, and device. Simply put, a user's actions may be a better indicator than who they report they are. Behavioral analysis is also key to detecting new fraud schemes and attacks that are not yet exposed.

When it comes to behavioral analysis, data worth considering include user interface browsing, account log-in behavior, physical biometrics, device interaction data, mobile fingerprint data, and geolocation behavior. Non-monetary data of interest may include a change of address, a request for a duplicate card, or a recent password reset. Spend velocity (the hours and days when someone tends to interact) and the time period between geographically dispersed payment locations are also details to consider. The growing shift towards streaming insights means that a customer's suspicious behavior that veers too far from the profiled norm can be singled out as fraudulent at an early stage – without the delay involved in point-and-click exploration.

Benefits for FIs and Merchants

- Detect new fraud schemes and attacks that are not yet exposed
- Greatly speed up fraud detection and response times (combined with rules-based alerts and machine learning)

INETCO'S CLIENT SUCCESS: PT. ALTO Network (ALTO) fraud risk team can use INETCO Insight's configurable machine learning models for more precise risk scoring and faster fraud pattern detection. These models were built to ingest transaction data in real-time, rebuild individual customer models on the fly, and assign a risk score for every transaction in milliseconds. Customer activity is continuously assessed and compared against set rules and predisposed behavior. INETCO Insight can also be integrated with ALTO's network firewall, sending automated action scripts that trigger the action of blocking suspicious transaction activity immediately.



7. Case management and automated workflows

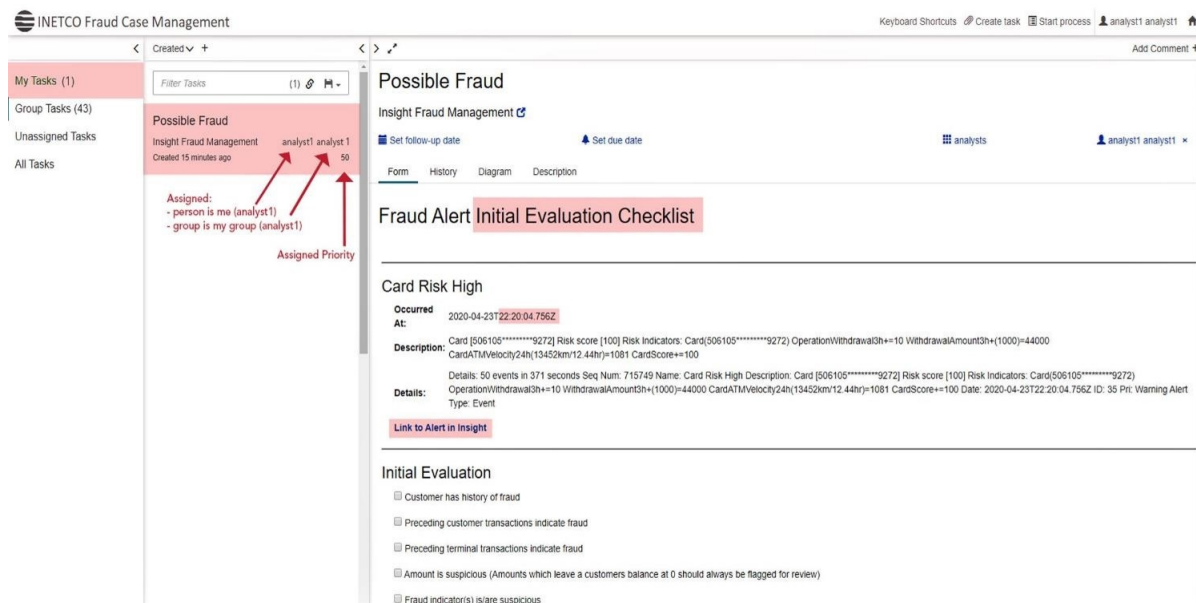
Case management and automated workflows are used to speed up triage and close payment fraud cases more efficiently. They help create a one-stop view of the incident summary, incident details, and fraud category displays. Workflow steps, escalation rules, and checklists can be configured to improve both the reactive investigation and proactive investigation of flagged fraudulent transactions. Access

Benefits for FIs and Merchants

Speed up triage and close payment fraud cases more efficiently

roles can also be defined and multi-layer reviews and approval processes enabled. Incident updates and audit trails are created with payment transaction profile specifics linked directly to each task, making it easy to determine if prior incidents have occurred with the customer. Human approval and decline decisions are also fed into machine learning fraud risk scoring models as they become available.

INETCO'S CLIENT SUCCESS: Here's an example of what happens when an alert triggers a task in INETCO's fraud case management system.



The screenshot displays the INETCO Fraud Case Management interface. On the left, a sidebar shows 'My Tasks (1)', 'Group Tasks (43)', 'Unassigned Tasks', and 'All Tasks'. The main area is titled 'Possible Fraud' and includes a 'Filter Tasks' dropdown. A task card for 'Possible Fraud' is highlighted, showing it was created 15 minutes ago and assigned to 'analyst1 analyst 1' with a priority of 50. Red arrows point to the assignment details: 'Assigned: - person is me (analyst1) - group is my group (analyst1)'. The task card also has a 'Set follow-up date' and 'Set due date' option. Below the task card, the 'Initial Evaluation Checklist' is visible, listing several criteria for evaluation, such as 'Customer has history of fraud', 'Preceding customer transactions indicate fraud', 'Preceding terminal transactions indicate fraud', 'Amount is suspicious (Amounts which leave a customers balance at 0 should always be flagged for review)', and 'Fraud indicator(s) is/are suspicious'.

The moment a real-time fraud alert is triggered in INETCO Insight, a case is automatically opened in INETCO's fraud case management system. At this point, a fraud analyst can claim that task and start working on it. The analyst is provided with details on why the alert was triggered, eliminating guesswork and improving employee's productivity. In this case, we can see that this was triggered because the card risk score is high, mainly due to the withdrawal amount and the distances between the usage points of this card, or velocity, being higher than normal.



8. Open APIs and fraud orchestration

Open APIs and fraud orchestration capabilities help eliminate siloes, avoid alert overload and optimize fraud management operations through the coordination of decisions from a single platform or hub.

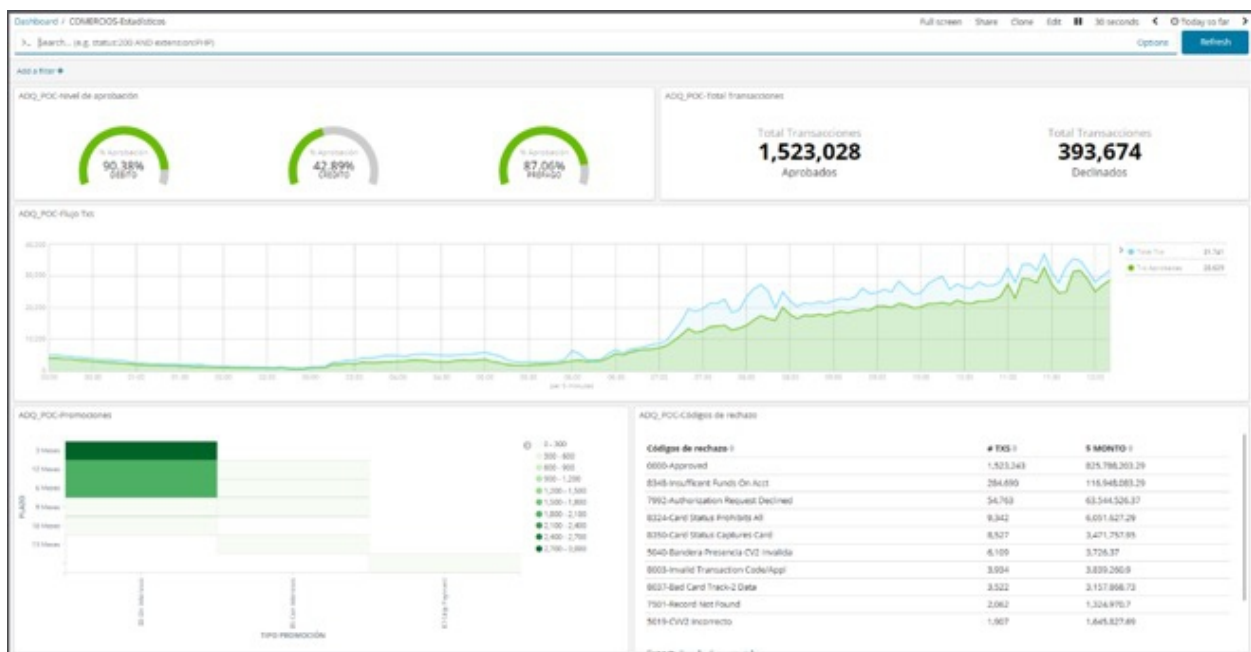
According to a December 2019 report released by the Aite Group^x, 36% of financial institutions surveyed said they had already implemented hubs, up 11% on the previous year. Multiple points solutions, a complete profile of every transaction and internal customer data is consolidated to optimize payment fraud detection, and prevention. This allows organizations to benefit from the capabilities of multiple fraud vendors while keeping operational costs under control and increasing agility in the face of evolving threats.

Benefits for FIs and Merchants

- Benefit from the capabilities of multiple fraud vendors while keeping operational costs under control
- Increase agility in the face of evolving threats

INETCO'S CLIENT SUCCESS: One of our clients, E-Global, the largest electronic payments processor in Mexico uses ODA to deliver INETCO Insight data to their own in-house fraud system.

Here's a real-time analytics dashboard that E-Global shared at the RBR event in London in 2019.



In this single dashboard, you can see real-time analysis of:

- approvals by card type,
- approved and declined totals
- declines by code totaled by volume and value

How INETCO Insight leads the way in payment fraud detection

Designed specifically for payment environments, **INETCO Insight was built to simplify real-time fraud screening - across all rails and channels.** The software platform eliminates detection lag times by overcoming the number one pain point of harnessing internal data effectively.

INETCO Insight's unique data collection happens out of band and directly off the network, meaning "in-flow" transactions are analyzed at each link of the end-to-end payments journey – invisibly, without any impact to the payment switch, traffic load, or speed. This is the only payment fraud solution to provide a one-stop view into both the network communications events and the application payload details of every transaction, a comprehensive view that is a must-have when it comes to detecting and preventing today's multi-vector payment fraud attacks.

INETCO Insight is a complete solution that brings together all 8 components detailed in this whitepaper: Omni-channel transaction data collection, real-time event monitoring, end-to-end transaction profiling, rules-based alerting, evolving machine learning, behavioral analysis, case management, and fraud orchestration. This cost effective software platform allows financial organizations, payment service providers, and retailers to:

- Assess the risk of every payment transaction in milliseconds – regardless of the customer endpoint or payment rail
- Precisely block transactions before major reputational damage or financial loss occurs
- Reduce customer friction and declines associated with false positives and outdated risk scores
- Enhance operational efficiency through case management and automated workflows
- Identify malware attacks, bot attacks, account takeovers and suspicious transaction activity from one platform
- Proactively identify and investigate new payment fraud patterns
- Integrate real-time transaction-level fraud detection and prevention tactics into a fraud orchestration hub of choice

The INETCO Insight payment fraud detection and prevention platform is deployed by banks, credit unions, retailers, card networks, and payment service providers in over 35 countries to detect payment fraud in real-time as well as prevent it.

"Payment fraud is greatly under-regulated in Indonesia. Together, with world-class partners such as INETCO, we can actively work to prevent card-present and card-not-present fraud attacks. We want to make customers feel safe when it comes to digital payment migration and help our member banks protect themselves against financial loss and a tarnished reputation – neither of which can be easily recovered." – PATRICCO BARON, CTO, PT. ALTO NETWORK [Read the Full Case Study](#)^{xi}

[See how E-Global, the largest electronic payments processor in Mexico, used INETCO Insight to quickly isolate operational performance issues, prevent fraud, and share data between IT operations and fraud teams faster.](#)^{xii}

Summary

When it comes to the state of digital payments today, nothing is static. The ongoing challenge is to keep customers safe against the evolving tactics of payment fraudsters – and to earn the level of trust you need to grow your payments business. This means your attempt to increase security should not lead to increased false positives and friction for customers.

Keeping pace requires an ongoing reassessment of your payment fraud management framework and an in-depth evaluation at every step of the customer payment journey. Armed with the right payment fraud detection and prevention software, you can defend against a variety of automated and human attack vectors, and enhance the security of every end-to-end payment.

Endnotes

- i. Rooney, K. (2020, April 29). Contactless payments Jump 40% as shoppers fear germs on cash and credit cards, Mastercard says. CNBC <https://www.cnbc.com/2020/04/29/mastercard-sees-40percent-jump-in-contactless-payments-due-to-coronavirus.html>
- ii. Montez, T. (2020, June 9). The Rise of Digital-First Banking <https://aitegroup.com/report/rise-digital-first-banking>
- iii. Montez, T. (2020, June 9). The Rise of Digital-First Banking <https://aitegroup.com/report/rise-digital-first-banking>
- iv. Yash, C. (2020, March 24). How do you stop payments fraud with the CARTA approach? <https://securityboulevard.com/2020/03/how-do-you-stop-payments-fraud-with-the-carta-approach/>
- v. Julie C. (2019, April 25). Entity Resolution and Linking: Enabling Next-Generation Financial Crime Detection <https://www.aitegroup.com/entity-resolution-and-linking-enabling-next-generation-financial-crime-detection>
- vi. INETCO. (n.d.). Moneris Solutions – Monitoring payment applications in over 350,000 merchant locations. INETCO. <https://www.inetco.com/resources/case-studies/moneris-solutions-monitoring-payment-applications-in-over-350000-merchant-locations/>
- vii. INETCO. (n.d.). How a Major Financial Institution in Africa Improved Early Warning Fraud Detection at the ATM. INETCO. <https://www.inetco.com/resources/case-studies/atm-fraud-detection/>
- viii. INETCO. (n.d.). How BECU Enhances Member Experience with Real-time ATM Transaction Intelligence. INETCO. <https://www.inetco.com/resources/case-studies/how-becu-improves-member-experience-with-real-time-atm-transaction-intelligence/>
- ix. Julie C. (2019, December 4). Fraud, Authentication, and Orchestration Hubs: A Path to Greater Agility <https://www.aitegroup.com/report/fraud-authentication-and-orchestration-hubs-path-greater-agility>
- x. INETCO. (n.d.). How PT. ALTO Network Provides World-Class Payment Transaction Security. INETCO. <https://www.inetco.com/resources/case-studies/pt-alto-network-end-to-end-payment-transaction-security/>
- xi. INETCO. (n.d.). Fraud Analytics Case Study: How E-Global Speeds Up Fraud Analysis and Improves IT Operational Performance. INETCO. <https://www.inetco.com/resources/case-studies/e-global-fraud-analytics-and-operations-performance/>

Focus on building your customer relationships. We'll protect them.



INETCO is a global fintech company that helps financial institutions, payment service providers and retailers unlock the full potential of their payment transaction data and prevent payment fraud. Headquartered in Vancouver, Canada, the company offers INETCO Insight® - a real-time transaction monitoring and analytics platform that was built specifically for payment ecosystems. With the unique ability to provide a true real-time audit of every link along an end-to-end payment transaction journey, INETCO Insight® has been deployed by a number of leading banks, payment service providers and retailers in over 35 countries.

Tech Mahindra

Tech Mahindra represents the connected world, offering innovative and customer-centric information technology experiences, enabling Enterprises, Associates, and Society to Rise™. We are a USD 5.1 billion company with 131,500+ professionals across 90 countries, helping 946 global customers including Fortune 500 companies. Our convergent, digital, design experiences, innovation platforms, and reusable assets connect across a number of technologies to deliver tangible business value and experiences to our stakeholders. Tech Mahindra is the highest ranked Non-U.S. company in the Forbes Global Digital 100 list (2018) and in the Forbes Fab 50 companies in Asia (2018). Tech Mahindra is part of the USD 21 billion Mahindra Group that employs more than 200,000 people in over 100 countries. The Group operates in the key industries that drive economic growth, enjoying a leadership position in tractors, utility vehicles, after-market, information technology, and vacation ownership.

Connect with us on www.techmahindra.com



+1.604.451.1567 | info@inetco.com | www.inetco.com