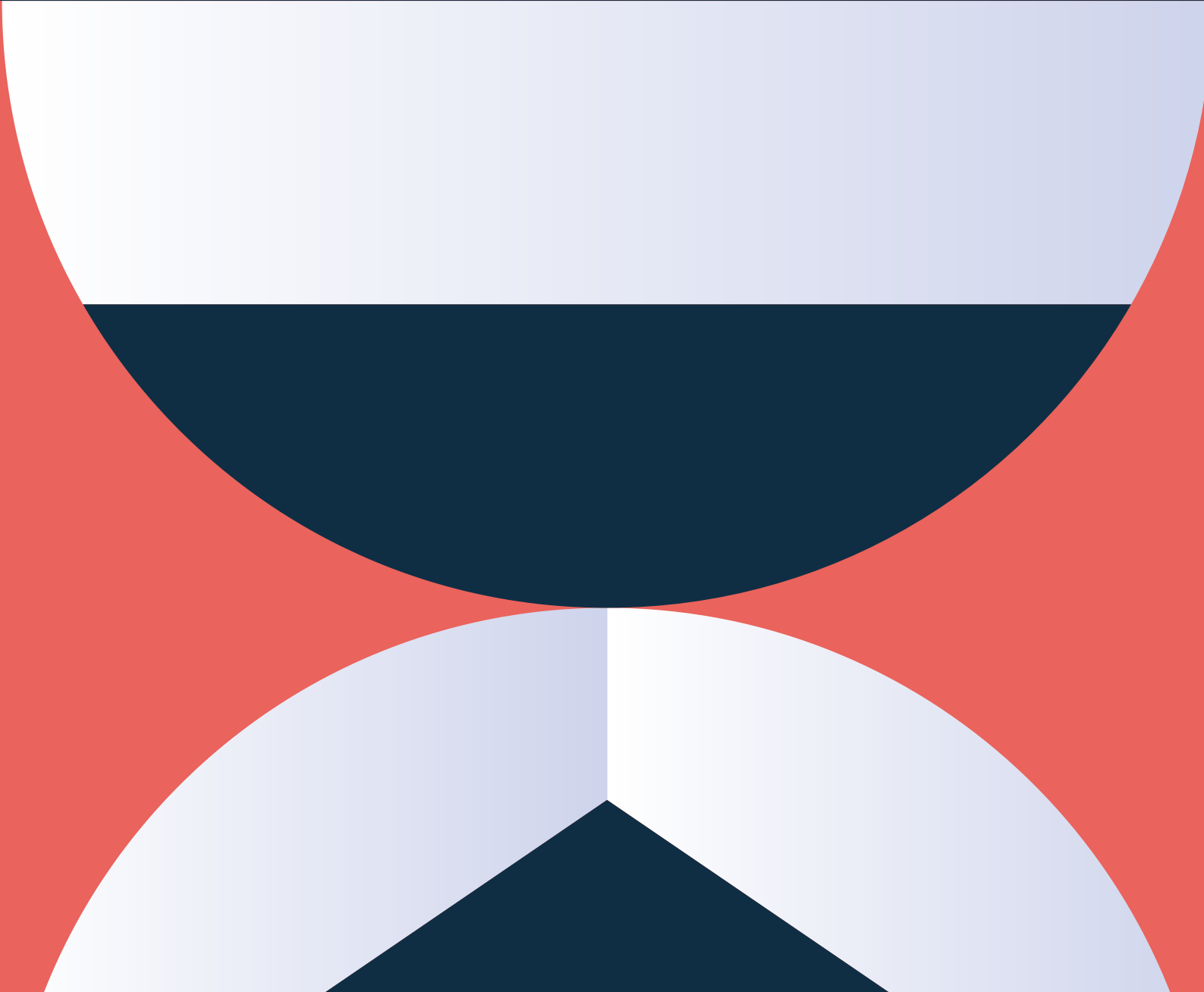


# Unit21

## SWITCH GUIDE

Fraud Detection Cannot Wait 24 Hours: What Real-Time Prevention Can Do For Your Fraud Strategy.



## PART 1

# The Current State: Time is Money

With the digital financial landscape innovating at breakneck speed, so too are fraudsters who are using every trick in the book to exploit this growth. Taking advantage of unprecedented collaboration, unlimited budgets, and advanced technology like AI and social media, fraudsters have become more savvy than ever. And with the explosion of faster payments - global real-time payment (RTP) transactions are predicted to reach 511.7 billion by 2027 - speed is also becoming a crucial component of fraud, both for those committing it and those detecting and preventing it.

## What can happen in 24 hours?



362,451

babies are born around the world



50-100

Hairs are shed by the average person



375M

hamburgers are eaten by Americans on the 4th of July



500,000

wire transfers are handled by FedWire



82M

Transactions are processed by The ACH Network



100

fraud attempts for a smaller institution on average



345,600

transactions are processed at 250-millisecond

## A Brief History

Of course, transaction monitoring for fraud prevention and anti-money laundering is nothing new. The concept of transaction monitoring that the world is familiar with today began gaining traction in the 1970s when most of the focus was on monitoring large cash transactions. But as banking offerings transitioned and new technologies came on board, such as new payment rails and new transaction types, this monitoring started to move more toward transaction monitoring, understanding how customers were behaving, and flagging any suspicious, out-of-character, or high-risk activities.

Today, transaction monitoring systems have become highly advanced. Combining sophisticated rules-based engines with AI and machine learning, these monitoring systems are quite different from the old days. But despite these great advances in technology, the numbers are still overwhelming when it comes to fraud. Global money laundering hit \$3.1 trillion and losses to global fraud were more than \$485 billion in 2023 - and this was just what was reported.

## The Time is Now

Clearly, there is a lot of room for improvement, both on the regulatory and FI side.

It's a fine line to walk. Those fighting fraud can be, understandably, risk averse. Adopting new systems can feel like a long, laborious process, creating additional risk. But with the FTC reporting that in 2023, U.S. fraud losses totaled \$10 billion (\$1 billion more than the prior year despite the number of cases remaining the same) staying still in fraud prevention is no longer a risk FIs and fintechs can take.

It's time for a change. There's no need to rely on processing flows that leave exploitable gaps for fraudsters. The moment of crisis is no longer an acceptable time to act; it's far too late. Adopting a fast, flexible, and precise platform designed to handle today's risks before they become tomorrow's losses is now more important than ever.



SUCCESS STORY WITH SALLIE MAE

### Out with the Old, In with the Wow

Strategic Approaches to Future-Proofing Fraud and Compliance

*Switching to a new technology provider can be daunting, even as more and more FIs realize they need to update their fraud and AML compliance tools. Watch our webinar on strategic approaches to future-proofing fraud and compliance, when experts from **Sallie Mae** and **Q2** will discuss:*

- **Understanding the Triggers:** Identify the key factors that drive financial institutions to switch technology providers and how to recognize when it's time for a change.
- **Strategic Implementation:** Learn best practices for transitioning to a new technology stack, ensuring minimal disruption and maximum impact.
- **Future-Proofing:** Discover how to select partners and tools that will help your institution stay ahead of emerging fraud and compliance challenges.

Watch now →

## PART 2

# The Challenges for Household Brands

The good news about today's fraud and AML detection and prevention is that there is robust technology available to help risk teams identify where fraudsters are and what they are doing. The goal now is to stop them before or during fraudulent activity.

While many legacy vendors are able to help organizations do this, it comes at a very high cost - monetarily, operationally, and reputationally. Their limitations tend to include:

- Offering only 24-hour batch processing, which is far too long in this current fast-paced landscape.
- Products with challenging integration with rigid workflows and data mapping.
- Little-to-no flexibility with rule building, effectively pigeonholing FIs into rules that may not be applicable or effective.
- Rigid workflows that require reliance on engineering/IT teams with even the smallest of technical changes.
- Inability to react to faster payments, exposing FIs to more fraud.
- Trouble accessing the right, timely data, which is usually siloed across countless tools.
- Inefficient investigations that take far too long to investigate with far too many false positives.

## Top Priorities for Risk and Compliance Teams in 2024



71%

Automating manual processes



64%

Improving efficiency & reducing costs



65%

Responding to new fraud schemes or regulations

Financial organizations need a solution that is faster for batch processing, has more flexibility in data mapping and rule creation, an implementation that doesn't constantly require operational and technical support - and for a cost that doesn't break the bank.

**Remember: fraud doesn't wait 24 hours. Next-day fraud detection is a day too late.**

## PART 3

# Making the Safe Bet vs. the Best Bet

Legacy players have in the past played an important part in the world of fraud detection and the AML space. Unfortunately, their very nature has made it difficult for them to evolve and grow to meet this new world of sophisticated, tech-driven fraud that FIs and fintechs are facing. In order for risk teams to effectively combat fraud in an impactful and sustainable way, they need a solution that sets them up for success now - and in the future:

- **Real-time resolutions:** Don't wait for processing flows that leave exploitable gaps for fraudsters; rely on real-time transaction monitoring to prevent fraud before it happens, reducing fraud losses.
- **Prescriptive yet flexible rules:** Out-of-the-box rule templates with dynamic properties and a visual flow empower risk teams to address flash fraud events without waiting for IT & engineering resources.
- **Artificial Intelligence everywhere:** Fraudsters aren't the only ones able to leverage AI. Optimize every step of the process with AI/ML-tuned models, workflow automation, and investigation checklists that reduce alert resolution time while increasing accuracy.



# Monitoring Speeds: What's the Difference?

Simplified, fraud prevention is the function of visibility and control. What is the speed at which organizations can detect fraud when it happens, and when it is detected, what can they do about it?

Generally, most financial organizations fall into three categories:

- **Traditional Monitoring:** Relying on a delayed response and typically using legacy vendors brought on board 15-to-20 years ago with alerts batched every 24 hours or the next business day. By default, they are in a very reactive state, with low visibility and low control.
- **Enhanced Transaction Monitoring:** Relying on rapid response. Usually, these are more forward-thinking FIs that understand it's prohibitively costly and timely to deploy a fully real-time solution to address every single transaction or potentially high risk due to technical, infrastructure, back-end, or even manpower challenges. However, they still want to ensure they can proactively fight financial crime and have a rapid response, generating alerts within fractions of 24 hours, resulting in higher visibility and control.
- **Real-Time Monitoring:** Focusing on immediately preventing high-risk or non-reversible transactions. They want to understand what the highest risk is for all inbound and outbound channels and ensure they can take action in real time when there is an alert, especially for high-risk transactions.



## Delayed Response

### Traditional Monitoring

Alerts delivered in **batches 24 hrs** after the transaction occurs

**Best for:** Slower-moving fraud or lower-risk channels

**EXAMPLE**  
**Wire Transfer**

**Use Case:** Monitoring for large sums being wired, especially internationally.

**Why Delayed Works:** Wire transfers often have settlement windows, making it possible to catch fraudulent activity even within a 24-hour window.



## Rapid Response

### Enhanced Transaction Monitoring

Alerts delivered as **fast as an hour**

**Best for:** Moderately urgent channels or fraud types

**EXAMPLE**  
**Account Takeover**

**Use Case:** Suspicious activity like abnormal login attempts or cred stuffing.

**Why Rapid Works:** A timely alert can stop attackers from accessing and draining funds or conducting further fraudulent actions.



## Lightning Response

### Real-Time Monitoring

Alerts in less than **250 milliseconds**

**Best for:** High-risk, high-velocity fraud channels

**EXAMPLE**  
**Instant Payments**

**Use Case:** Fraud detection for instant payments like Zelle or FedNow

**Why Instant Works:** Instant payments are completed within seconds, so real-time alerts are necessary to prevent fraud before the funds leave the account.

With the payment rails continuing to get faster, organizations' core strategies should no longer be in the delayed response category. In these times, there is no reason anyone should wait 24 hours for an alert to be generated so it can be investigated after the fact. While there might be a few use cases in which the delayed response category is acceptable (e.g., outbound wire transfers), most FIs and fintechs want to generate alerts as close as possible to the transaction point to prevent fraud losses. And if the technical capabilities and right risk appetite exist, the channels and transactions associated with the highest liability will ideally be monitored within the lightning response category.

As the evolution of the payments landscape and fraudsters themselves continue to grow, so too is the evolution of the transaction monitoring speed. Traditional monitoring is no longer good enough to meet the demands of today's risk teams to effectively fight fraud.



## PART 4

# The Value of the Unit21 Solution

Unit21 provides a faster, more flexible, and cost-effective solution compared to well-known legacy providers by providing two core offerings:

 **Asynchronous rule engine - designed to monitor fraud**

 **Real-time rule engine - designed to prevent fraud**

The asynchronous engine that provides transaction monitoring capabilities is a rule engine that solves the pain points FIs and fintechs deal with today, such as siloed data, inefficient rules, heavy reliance on engineering resources, and long and repetitive manual reviews. This rule engine sets out to ensure risk teams have all the data available to them to make the best possible decision in the shortest amount of time.

With real-time monitoring capabilities, responses can be provided in 250 milliseconds and fraud can be stopped at the time of the transaction. Procedures can be automated after being manually built, but actions such as white labeling legitimate customers can also be done to reduce the amount of false positives.

## Legacy Vendors vs. Unit21 Capabilities

### LEGACY VENDORS

Struggles to keep pace with faster payments, which exposes organizations to more fraud; resolve and process in a 24-hour batch processing.

Has trouble accessing the right, timely data. Needs access to more and new data, which is siloed across countless tools.

Unable to implement new or edit existing rules. Poor rule writing leads to greater inefficiency and boxed-in scenarios.

Takes far too long with inefficient investigations that result in far too many false positives.

### /// Unit21

Offers real-time monitoring (RTM) and faster resolutions; resolve and process in <250 milliseconds. That's less than 0.0003% of a 24-hour timeframe.

Supports simple, flexible data integration options with white-glove service that prioritizes needs and success.

Finds the best rules applicable to an organization's goals, allowing them to set their own thresholds and filter on the data they want.

Effectively and efficiently leverages AI with checklists and workflow automation based on fraud typology.

Unit21 takes a preventative approach with real-time monitoring, stopping suspicious transactions before they lead to loss. With full model explainability and all historical and related data available in a visual dashboard, analysts can be confident in their decisions. Everyone on the team is empowered to do it themselves with a simple, no-code interface and rules for common scenarios that are available out of the box.



## PART 5

# Worksheets and Tools to Get Started

### Lineup internal resources

Unit21 offers structured onboarding & implementation support to make this process easier.

### Data Migration

Unit21's flexible APIs & customizable integrations can make data migration seamless, based on real-world onboarding examples

### Align on metrics & KPIs

Defining KPIs creates vital tools for measuring the effectiveness and efficiency of fraud prevention and detection efforts within an organization.

## Develop KPIs

KPIs provide quantifiable metrics that allow the organization to assess the impact of their fraud management strategies, identify areas of improvement, and make data-driven informed decisions. Five goals organizations can achieve by defining KPIs:

- **Performance Evaluation:** KPIs provide the ability to evaluate the performance of a fraud management system.
- **Early Trend Detection:** KPIs help organizations identify suspicious patterns and anomalies in near real-time.
- **Resource Allocation:** Organizations can use these metrics to determine where to allocate resources effectively.
- **Continuous Improvement:** Regularly monitoring and analyzing KPIs encourages organizations to make changes where needed to evolve with fraud.
- **Risk Mitigation:** By measuring the program in place, you can maximize revenue from safe customers, focusing your efforts and increasing friction points for suspicious users.

## Sample KPIs

Some useful KPIs include, but are not limited to:

### Fraud Detection KPIs

- Number of fraud incidents detected per month.
- Detection fraud rate (%): Ratio of detected fraud alerts to total suspected alerts.
- False positive rate (%): Percentage of non-fraudulent alerts misclassified as fraud.

### Fraud Prevention KPIs

- The number of proactive measures implemented.
- \$ Value associated with True Positive alerts.
- Percentage of blocked fraudulent transactions.

### Investigation & Resolution KPIs

- Average time to resolve a fraud alert.
- Rate of successful fraud case resolution.
- Customer satisfaction after fraud resolution

### Operational Efficiency KPIs

- Manual intervention rate (%).
- Alerts per agent per day/week/month.
- Time spent per case for manual reviews.

### Financial Impact KPIs

- Total financial losses due to fraud.
- Losses per payment rail.
- Recovery rate (%): Amount of money recovered from fraud cases.

### Counts and Trends

- Total Alerts / Total Cases / Total SARs filed
- Active AML Rules
- Highest / Lowest Performing Rule

### AML Program Effectiveness KPIs

- False Positive Rate
- Alert to Case Ratio
- Case to SAR Ratio

### Team Efficiency KPIs

- Average Handle Time: Alerts
- Average Handle Time: Cases
- Average Handle Time: SAR filing

### Customer Risk

- Customer Risk Rating: High
- Customer Risk Rating: Medium-High
- Customer Risk Rating: Medium

### Work Quality KPIs

- Alert work: Percentage Perfect / Good / Not Good
- Case work: Percentage Perfect / Good / Not Good
- SAR filing: Percentage Perfect / Good / Not Good

When evaluating vendors, make a short list of your teams must have features. Here's a quick checklist example:

**CAPABILITY**

- User control with customization

---

- Automation with AI

---

- Superior fraud monitoring with real-time and same-day monitoring

---

- Core agnostic: seamless integration with any core system

---

- Sanctions & watchlist functionality

---

- CTR reports automation

---

- Customer Risk Ratings (CRRs) in rules

---

- Ongoing Transaction screening

---

- Comprehensive rule library

---

- Dynamic rule building to create & customize rules quickly

---

- No-code rule builder

---

- Auto-assign or round-robin alerts/cases to analyst(s)

---

- Data migration from banking cores & other systems

#Unit21	COMPANY X
✓	—
✓	—
✓	—
✓	—
✓	—
✓	—
✓	—
✓	—
✓	—
✓	—
✓	—
✓	—

You'll want to make a more detailed checklist to compare your detailed requirements. Here is an example that you can leverage for your company:

KEY CRITERIA	Company X	Company Y Company Z
<b>REGULATORY COMPLIANCE &amp; AUDITABILITY</b>		
<p>Compliance with Key Regulations: The vendor must ensure that their solution complies with local and international regulations such as the Bank Secrecy Act (BSA), Anti-Money Laundering Act, FATF guidelines, and FinCEN rules.</p>		
<p>Audit Trails: Solutions should provide comprehensive, immutable audit trails for every transaction, alert, rule change, or case, ensuring traceability for internal and external audits.</p>		
<p>Regulatory Reporting: The ability to automatically generate Suspicious Activity Reports (SARs), Currency Transaction Reports (CTRs), and other compliance filings.</p>		
<p>Audit Trails: Solutions should provide comprehensive, immutable audit trails for every transaction, alert, rule change, or case, ensuring traceability for internal and external audits.</p>		
<b>REAL-TIME FRAUD DETECTION</b>		
<p>Speed of Detection: The ability to monitor transactions in real-time (preferably within milliseconds, as Unit21 offers) to prevent fraud before it happens, rather than detecting it post-event.</p>		
<p>Advanced Analytics and AI/ML: Use of machine learning models and artificial intelligence to detect emerging fraud patterns and adjust to new threats automatically.</p>		
<b>FLEXIBILITY &amp; CUSTOMIZATION</b>		
<p>No-Code/Low-Code Rule Building: The ability for non-technical teams (like compliance or risk teams) to create, test, and modify fraud and AML rules without the need for heavy IT involvement.</p>		
<p>Customizable Workflows: The solution should allow customization of alert and case management workflows to suit the organization's specific needs.</p>		
<p>Dynamic Model Building: The vendor should offer tools to build custom scenarios and models for fraud detection based on unique requirements and data.</p>		

KEY CRITERIA	Company X	Company Y	Company Z
--------------	-----------	-----------	-----------

**FALSE POSITIVE REDUCTION**

**Accuracy of Alerts:** A solution that can significantly reduce the rate of false positives, which helps minimize wasted resources and improves operational efficiency.

**Testing and Validation Tools:** The ability to test rules on historical data or run new rules in shadow mode before deploying them live to minimize operational risks.

**DATA INTEGRATION & COMPATIBILITY**

**Data Ingestion:** The solution must offer flexible integration options, such as APIs, to ingest data from various internal systems (e.g., core banking, transaction monitoring, KYC/KYB systems).

**Data Agnosticism:** The vendor should allow organizations to integrate diverse data types and sources, whether structured or unstructured, without requiring rigid data formats.

**Seamless Migration:** The ability to efficiently migrate data from legacy systems with minimal disruption.

**SCALABILITY & PERFORMANCE**

**Support for High Transaction Volumes:** The solution must be able to handle large transaction volumes efficiently, scaling as the organization grows.

**Cloud-Based and On-Premise Options:** Organizations should evaluate whether the vendor offers both cloud-based and on-premise deployments to match their operational preferences.

**EASE OF IMPLEMENTATION & INTEGRATION**

**Implementation Support:** Vendors should offer robust onboarding and implementation support to reduce friction and ensure a smooth transition from legacy systems.

**Speed of Deployment:** Evaluate how quickly the system can be deployed, tested, and fully operational, particularly for mission-critical compliance systems.

**Integration with Other Tools:** The vendor should offer pre-built integrations with other commonly used platforms (e.g., KYC, fraud management, identity verification) or provide API access for custom integrations.

KEY CRITERIA	Company X	Company Y	Company Z
<b>REPORTING &amp; DASHBOARDS</b>			
<p>Visual Reporting Tools: Vendors should offer user-friendly dashboards that provide insights into transaction trends, suspicious activity, rule performance, and team efficiency.</p>			
<p>Custom Reporting: The ability to generate custom reports tailored to the organization’s regulatory and operational needs.</p>			
<b>CUSTOMER SUPPORT &amp; SUCCESS</b>			
<p>Customer Support Quality: Evaluate the vendor’s support model, including response times, availability (e.g., 24/7), and the quality of ongoing support.</p>			
<p>Training and Knowledge Base: Look for vendors that offer comprehensive training, documentation, and ongoing educational resources to help teams make the most of the solution.</p>			
<p>Proactive Account Management: Vendors should provide dedicated account managers or customer success teams to ensure continuous optimization and performance of the solution.</p>			
<b>COST &amp; ROI</b>			
<p>Total Cost of Ownership (TCO): Consider the cost of the solution, including licensing, implementation, support, and future scalability. Also, evaluate whether the vendor’s pricing model is competitive and aligned with your budget.</p>			
<p>Return on Investment (ROI): Evaluate how the solution contributes to reducing fraud losses, operational costs, and compliance risks.</p>			

**PART 6**

# Start Fighting Tomorrow's Fraud Today

Don't let legacy systems dictate how you protect your institution. Why wait 24 hours for what you can do in 250 milliseconds? Our real-time monitoring ensures you stop fraud as it happens, not just detect it after the damage is done.

Unit21 is your dedicated partner in fraud prevention and compliance from implementation to ongoing support, and offers tailored support to guide you through the process.

Get a Demo →

