Unit21

White Paper: Real-Time Monitoring

Abstract

The mass adoption of real-time payments means money is moving faster than ever. This is great for individuals, businesses, financial institutions (FIs), government agencies, and the economy in general, but it's a major hurdle for risk management professionals.

With payments traveling virtually instantly, fraud is now happening just as fast, prompting risk management teams to adopt a real-time monitoring system that can keep pace. While RTM solutions aren't entirely new, the rise of real-time payments has made them more imperative than ever for anti-fraud operations.

In this report, we explore how real-time payments will impact anti-fraud operations in the coming years and provide expert advice on how risk professionals can navigate this changing landscape. Readers will leave having a deep understanding of the current state of the real-time payment market, how the rise of real-time payments will impact fraud prevention teams, and how real-time monitoring can be used as an effective tool for real-time payment rails, allowing for a safe and frictionless experience for end users.

Contents

The Current State of Real-Time Payments

Unit21

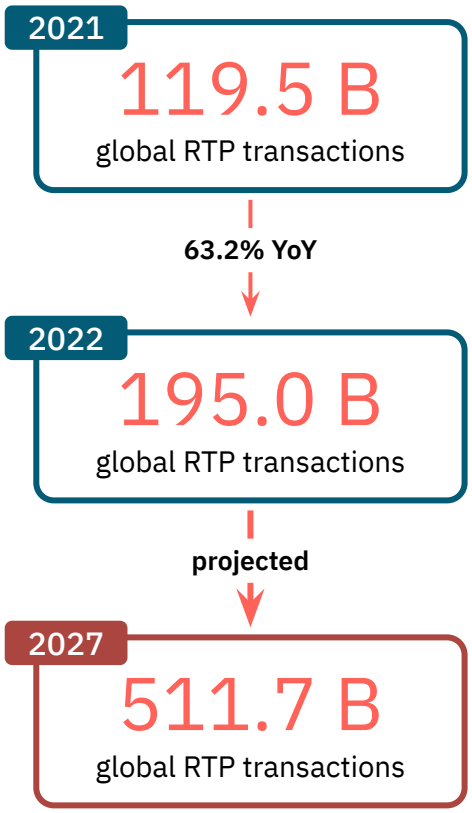
While real-time payments are by no means new, they have been growing in popularity recently as countries have begun integrating real-time payment systems into their national payment networks.

Below, we explore the state of the global RTP industry, with special focus on the U.S. market.

Global real-time payment market growing steadily

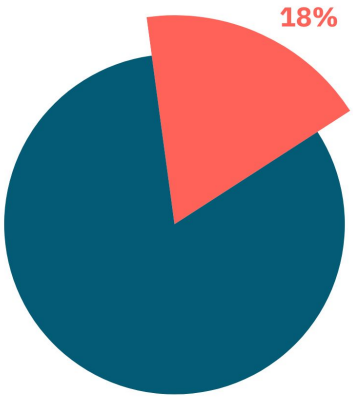
> "The journey to real-time for payments is an inextricable one and the obvious destination for all payments irrespective of whatever rail they travel on."
>
> - **Peter Hazou, Director of Business Development & Financial Services at Microsoft**

The prominence of real-time payments in the modern era is inevitable.



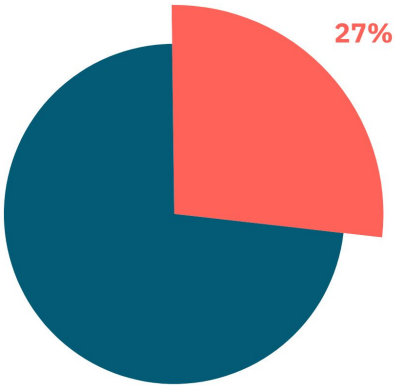
Data Source: It's Prime Time for Real-Time 2023, ACI Worldwide

According to ACI Worldwide's March 2023 report, real-time payments are supported by more than 70 countries, and real-time payments totaled $195 billion worth of transactions in 2022, 63.2% higher than in 2021. And—based on a CAGR of 21.3% between 2022 and 2027—this number is projected to hit $511.7 billion by 2027.



Real-time payments accounted for 18% of the gobal electronic payments market in 2022

Data Source: *It's Prime Time for Real-Time 2023, ACI Worldwide*



Real-time payments are projected to account for 27.8% of global electronic payments in 2027.

Data Source: *It's Prime Time for Real-Time 2023, ACI Worldwide*

Real-time payments have proven to be a major emerging competitor in the electronic payments sector globally, accounting for 18% of all electronic payments in 2022. This is anticipated to grow in the coming years, with ACI Worldwide anticipating real-time payments will account for 27.8% of the electronic payments sector by 2027.

Instant settlement options are gaining popularity. This trend is driven largely by options that empower B2B, B2C, and account-to-account transactions for businesses, financial institutions, and government agencies, rivaling P2P services for consumers.

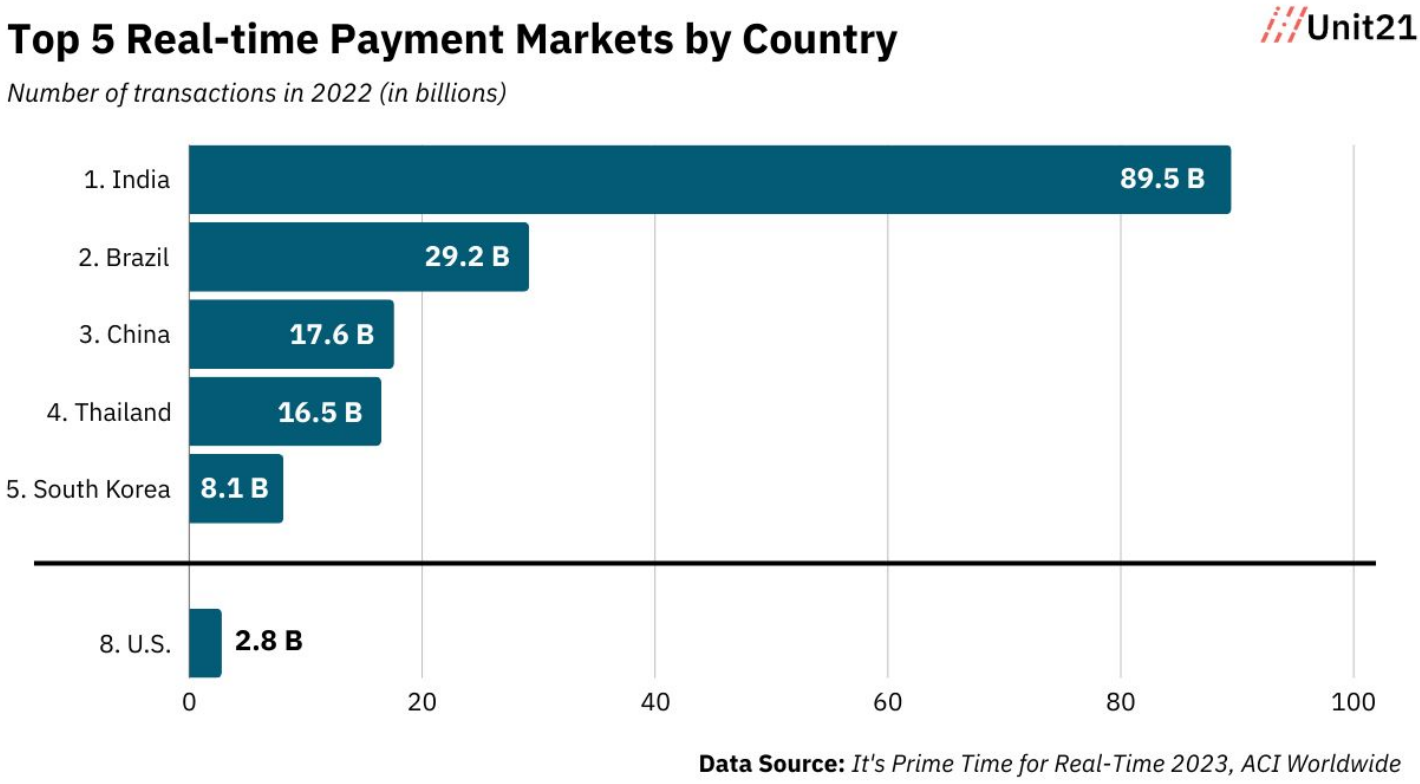
> "The real-time world around us is prompting the banking system to modernize its infrastructure and processes to accommodate real-time activities and the data that travels with them."
>
> **- Peter Hazou**

Globalization, accessibility, and a variety of other factors are driving a need for real-time payments.

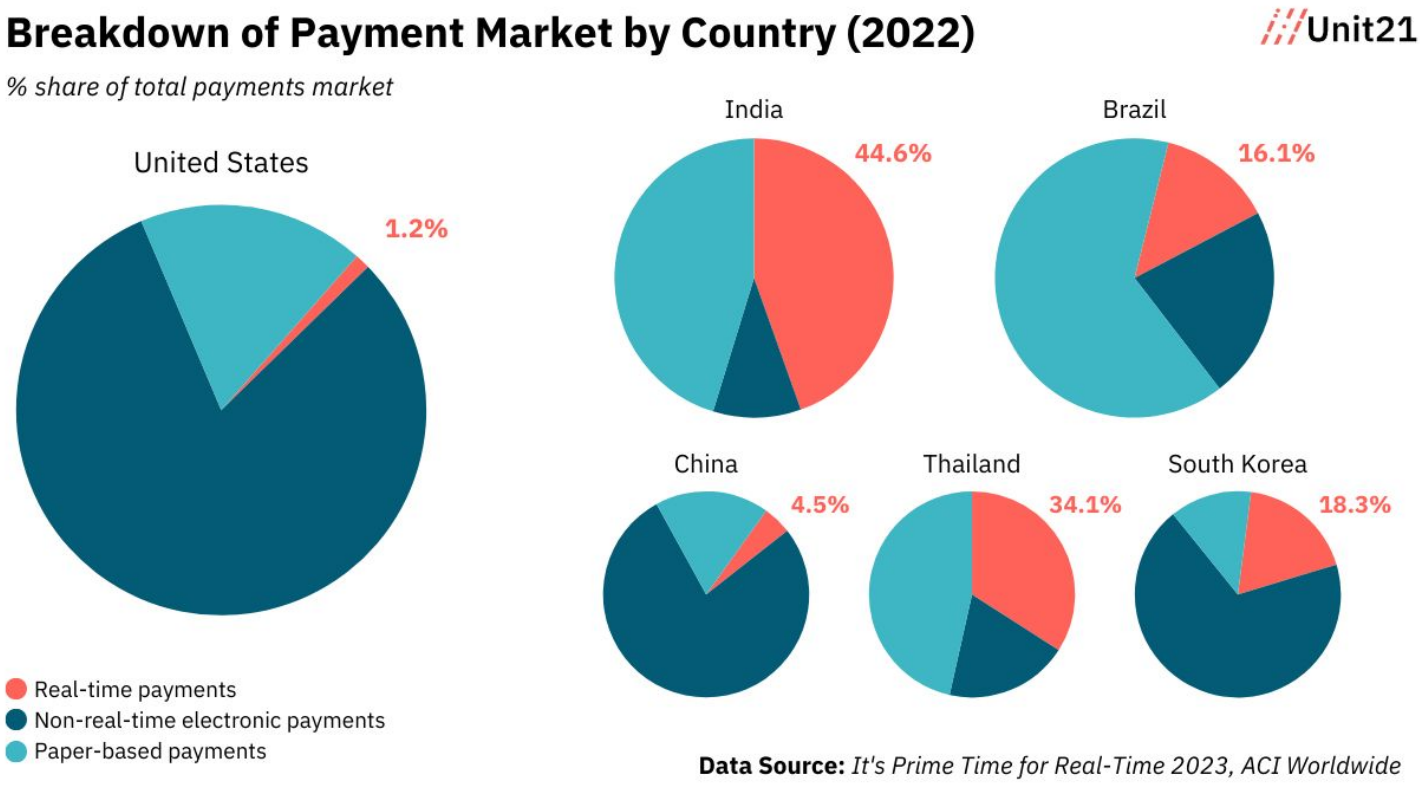
United States lags behind on the global stage

While global real-time payment adoption is steadily trending upward, the United States is behind the mark.

In 2022, the Asia-Pacific region had the most success in the real-time payment market, claiming a combined 41% of the global revenue. And there's a good reason for this success; four of the top five countries with the highest transaction volumes were in Asia-Pacific.



It's also no surprise that India and Brazil are leading the pack, as both have their own real-time payment networks that are regulated closely by government banking authorities—the Reserve Bank of India (RBI) and the Central Bank of Brazil (BCB). They've also been able to capture a larger part of their market, drawing users to real-time payments much faster and effectively than the United States.



The upside is that while the United States currently ranks 8th on the ACIs Worldwide's It's Prime Time for Real-Time 2023 report in terms of total real-time transaction volume, with only 1.2% of its payment market being penetrated by real-time marketing, there is plenty of room for growth. With the surge in RTP network interest following the launch of FedNow, the U.S. market should begin to expand aggressively in the coming years.

According to Grandview Research, "North America is expected to witness a steady growth rate over the forecast period [2023 - 2030]. The region is home to several prominent players in the global market "and an increase in the number of immigrants" is expected to increase the number of cross-border disbursements."

In short, with so many U.S. citizens already using electronic payments, the U.S. market is primed to see a real-time payment boom in the next five to ten years.

RTP networks begin to challenge batch processing for market dominance

In the U.S., there are two major RTP networks contending for their share of the real-time payments market: The Clearing House's RTP and FedNow.

	RTP	FedNow
Operated by	The Clearing House	Federal Reserve
Launched	November 2017	July 2023
Transactions	Credit "push" payments	Credit "push" payments
Revocability	Irrevocable	Irrevocable
Availability	24/7/365	24/7/365
Max transfer amount	1,000,000 USD	500,000 USD
Credit transfer fee	0.045 USD	0.045 USD
Request for payment fee	0.01 USD	0.01 USD

And while they are largely competing against each other to be the sought-after RTP network, they're also both competing together against the Automated Clearing House (ACH) as the dominant payment rail of the future.

Bolstering the real-time payment infrastructure isn't just about business though, it's also about pushing payment initiatives forward and nurturing the economy. As Senior Vice President of Real-Time Products at Mastercard, George Evers, says, "Established drivers, such as financial inclusion, remain as relevant as ever, but the role of real-time payments as a stimulus for economic growth will be higher in the minds of governments and regulators. It has been proven out that, combined with the perpetual motion of mobile utilization and the digitization of everything, real-time payment systems offer a foundation for economies to be more dynamic."

But these systems themselves aren't without change either. Currently, the on-premise market is thriving. According to Grandview Research, "the on-premise segment dominated the market in 2022 and accounted for a share of more than 60.0 of the global revenue." But as real-time payments improve and more companies invest, cloud-based and open banking infrastructures will advance as well, empowering payment infrastructures that can be even faster and more seamless.

FedNow fuels adoption of RTP networks

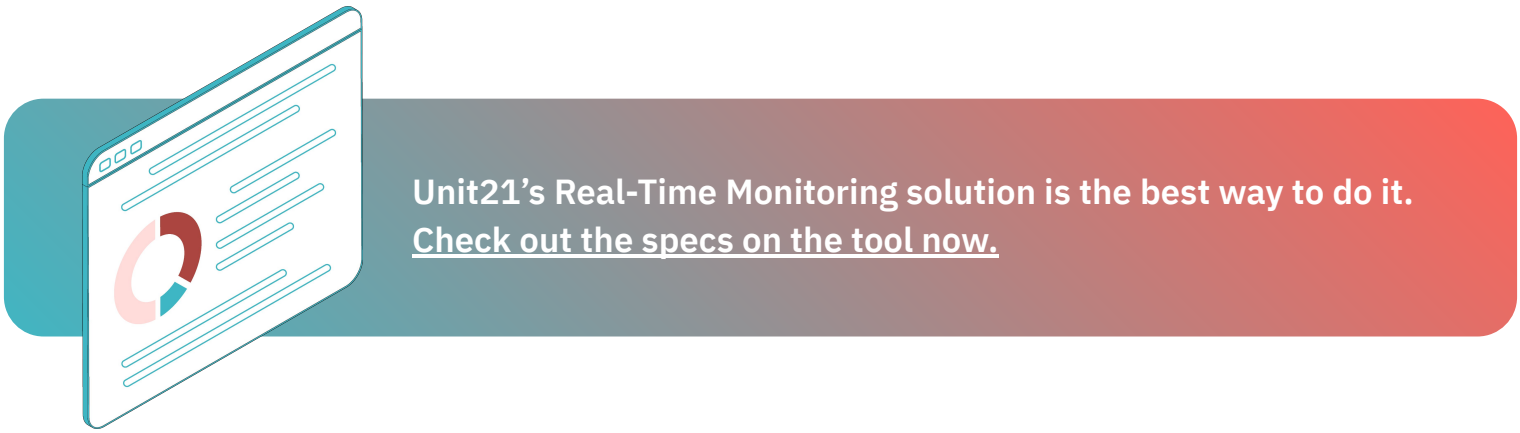
Real-time payment adoption in the United States has been lackluster, with The Clearing House's RTP network struggling to see significant growth since its launch in 2017, especially early on.

This slow development of the RTP offerings in the US has been partly due to slow adoption, partly due to fraud concerns and partly because of a market that was waiting to see what the Federal Reserve was planning to roll out, causing other contenders to wait. David Watson, CEO of The Clearing House noted that "we probably lost about five years as a country" as a result of major players in the industry deciding to step back and wait to see what developed before laying their own stake.

But in the last few years, the demand for real-time payments has been growing, a demand that is currently picking up pace as both the TCH and FedNow onboard more participants. According to PaymentsDive, a spokesperson for TCH said that "200 banks and credit unions have joined the RTP network" in 2023, with approximately "130, or two-thirds, jumping on board since July" of that year. They also claimed that since FedNow launched, they've started "onboarding four times as many banks to the RTP network."

While early adoption was slow, the push by the Federal Reserve to provide a government-backed real-time payment system parallels what other countries have been doing and has been motivating financial institutions to get on board. And with two real-time payment services in the market, there should be some healthy competition to be the top choice of financial institutions.

The global real-time payment market is growing, and the U.S. market is poised for significant growth as it plays catch up with leaders in the RTP space. Now it's up to risk management teams to keep up with the fraud that comes with it.



What Real-Time Payments Mean for Fraud & Risk Professionals

Unit21

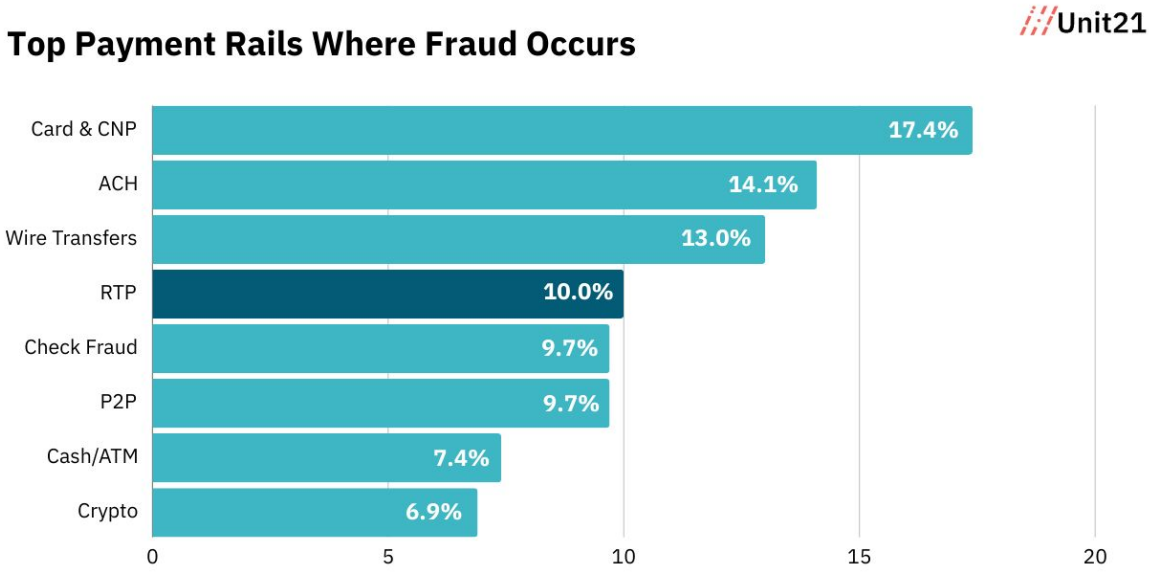
But what does all of this mean for fraud fighters?

A few core changes are happening in the fraud landscape, driven largely by real-time payments and the need for an around-the-clock monitoring solution.

1. Fraudsters are shifting their attacks to real-time payment rails
2. The window for intervention is becoming shorter, and
3. A new tactic is emerging against RTP rails - Authorized Push Payment (APP fraud)

We'll look at how these changes impact risk management operations and explore strategies for handling this cataclysmic shift in the payment market.

Fraudsters are shifting their attacks to real-time payment rails



Data Source: *State of Fraud and AML Report Volume 2, Unit21*

Real-time payment rails are lucrative to fraudsters for the same reasons they are appealing to users: they process and settle payments instantly and recipients get immediate access to funds. But what's even more appealing to fraudsters is that the payments are **irreversible**—especially when they've been legitimately authorized by the sender.

As real-time payment adoption rates rise, more fraudsters will flock from legacy payment systems like ACH, wire, and checks to real-time payment rails. According to our 2023 State of Fraud and AML Report, real-time payments have already become the fourth highest payment type experiencing fraud. And as more FIs shift portions of their services away from batch processing to real-time processing we'll likely see an even greater rise in fraud on real-time payment rails in the coming years.

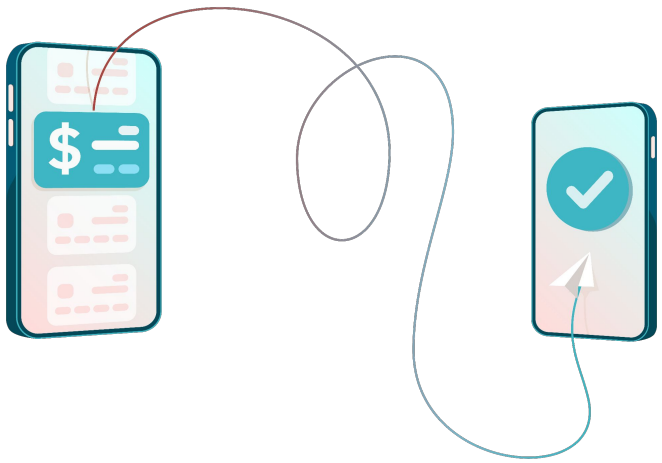
Real-time payments have a short window for intervention

While the push to real-time payment adoption could mean major benefits for financial institutions and end-users, the speed required for real-time payments poses problems for fraud teams looking to monitor these transactions.

> "The speed at which the world operates also creates a lot of uncertainty and risks which banks, and the payment systems they operate, are trying to accommodate."
>
> - **Peter Hazou**

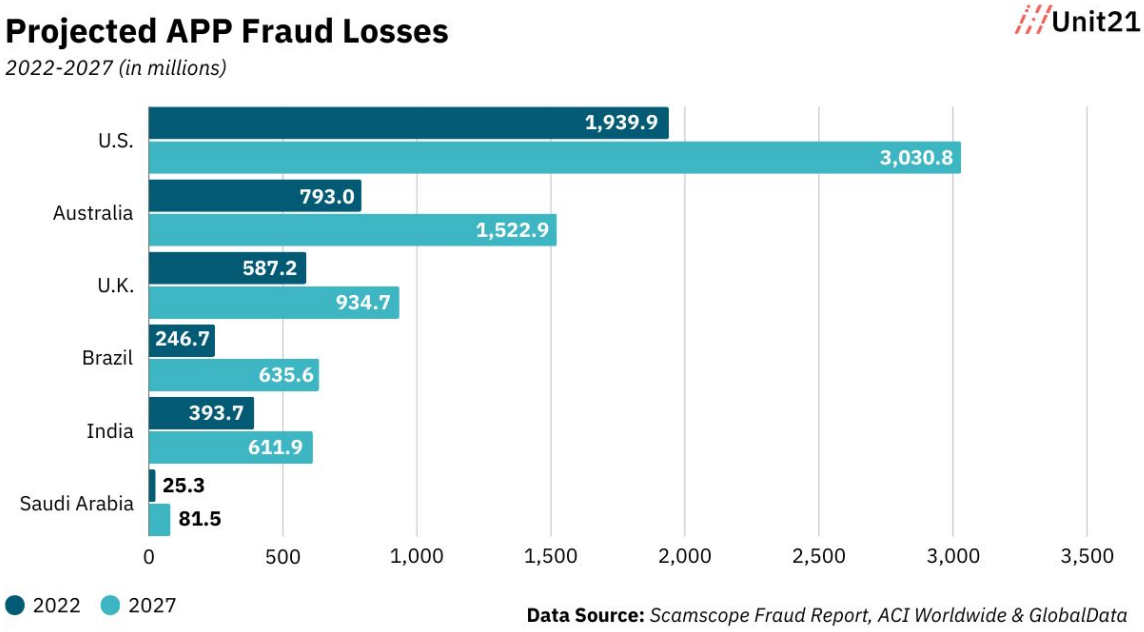
Using real-time monitoring drastically shrinks the window of action for risk teams, leaving them little time to alert on—let alone interdict—a transaction. When you're trying to settle transactions within seconds, latency problems can categorically inhibit your ability to act. And the more data integrations your system is using, the more room for error.

Even if your system can accurately and efficiently detect fraud and execute finely-tuned rules, if it can't do it virtually instantly, it simply won't help in the fight against real-time payment fraud.
It's imperative to ensure the real-time monitoring solution you deploy can process data without latency issues, integrating seamlessly with the rest of your risk infrastructure.

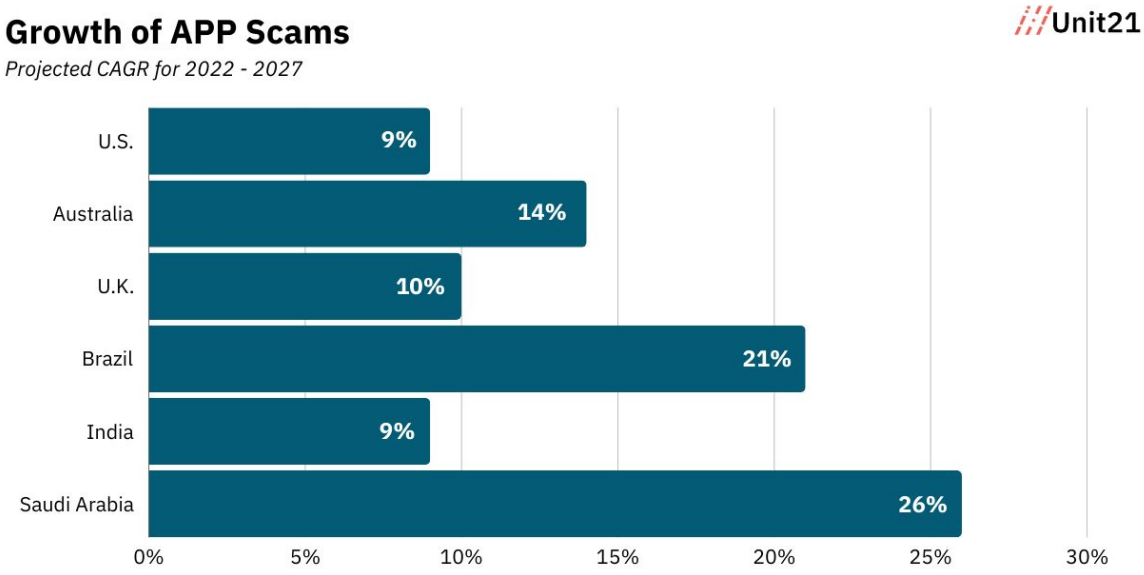


Authorized Push Payment (APP) fraud is a top tactic against RTP rails

Fortunately, fraudsters have just as short of a window to act as risk professionals do to stop them, limiting the tactics they can use to commit fraud. The only downside is that criminals have begun to hone in on—and perfect—fraud tactics that are most effective on real-time payment rails. And the leading—and growing—threat is Authorized Push Payment (APP) fraud, achieved largely through the use of social engineering and confidence tricks.



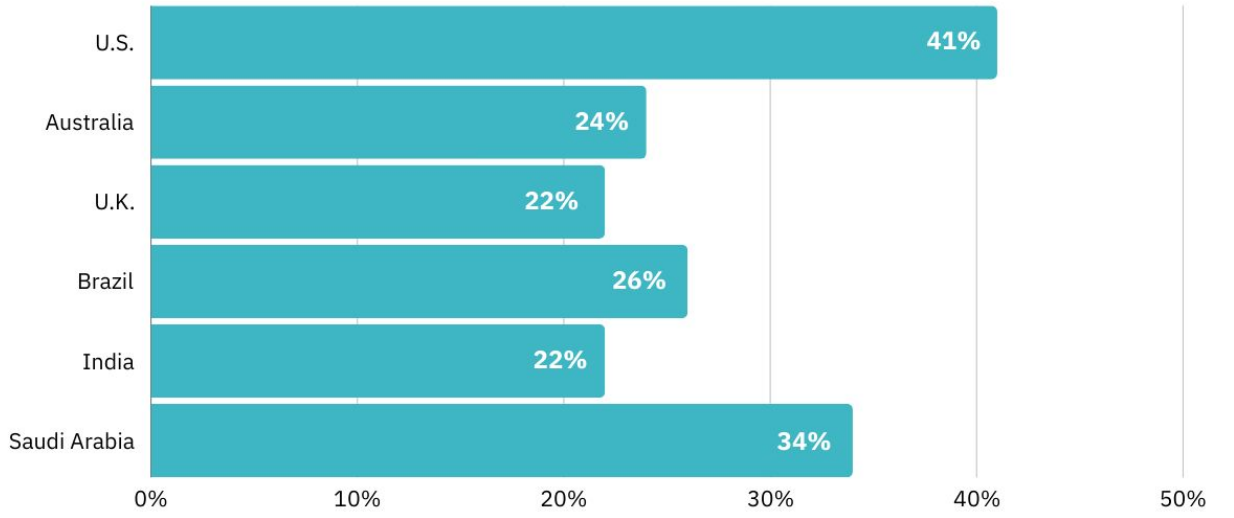
Data Source: *Scamscope Fraud Report, ACI Worldwide & GlobalData*



Data Source: *Scamscope Fraud Report, ACI Worldwide & GlobalData*

Growth of Real-Time Transactions

Projected CAGR for 2022 - 2027



Data Source: *Scamscope Fraud Report, ACI Worldwide & GlobalData*

According to an ACI Worldwide Scamscope Report, "Authorized Push Payment (APP) scam losses are on the rise and expected to climb to $6.8 billion—a combined compound annual growth rage (CAGR) of 11%—by 2027 across six leading real-time payments markets (U.S., U.K., India, Brazil, Australia and Saudi Arabia)." On its own, the United States suffered $1.9 billion in APP fraud losses in 2022, and this is expected to rise (at a CAGR of 9%) to $3 billion by 2027.

But what does this have to do with real-time payments?

APP fraud has always been appealing to fraudsters. Since the payment has been authorized, it raises less flags from FIs and leaves victims with less recourse to recover their funds. But real-time payment rails make APP fraud more appealing to fraudsters than ever because transactions are **instant** and **irreversible**. The payment settles instantly and the criminal gets immediate access to the funds.

> "APP scams pre-date real-time payments, but instant clearing, a strong supply of mule accounts, and successes tackling other types of fraud have made the "business case" stronger."
>
> **- Cleber Martins, Head of Payments Intelligence and Risk Solutions at ACI Worldwide**

As real-time payments adoption rates rise, APP fraud will follow suit. Effective real-time monitoring solutions like Unit21 have rules that look for suspicious activity or behavioral anomalies that could signal APP fraud or even an account takeover. Anomaly detection models can identify abnormal patterns based on historical deviation to root out transactions that would otherwise look legitimate.

> "The only way to turn the tide on APP fraud is if the initiating and receiving ends of transactions can collaborate—without sharing sensitive information about customers with competitors or breaching privacy regulations."
>
> **- Cleber Martins**

Here at Unit21, we agree. That's why we've developed the Fraud DAO, a data data consortium of fintechs and traditional FIs, that collaborate and share fraud strategies, mitigation tactics, and offenders to strengthen the fight against fraud.

Moving from Fraud Detection to Fraud Prevention with Real-Time Monitoring

Unit21

Until The Clearing House's RTP was introduced in 2017, the only payment settlement solution companies had was batching processing—of which ACH was the leading example.

But with batch processing, organizations are typically limited to detecting fraud after it's been committed because they aren't conducting any real-time monitoring. This means a series of fraudulent payments could be processed before an alert is generated and teams can act on the case.

With real-time monitoring, teams are no longer restricted to the reactive mindset of fraud detection and can instead leverage real-time information into proactive fraud prevention efforts.

When used properly, real-time monitoring can empower teams to:

- **Interdict suspicious transactions as they are in progress**
- **Identify a fraudulent card or account and restrict any future activity**
- **Quickly implement rules for recently detected fraud scenarios**

Real-time monitoring can stop real-time payment fraud, but it can also be used to stop future instances of fraud. For example, a stolen credit card could be used to make multiple purchases, but if real-time monitoring can alert on the first purchase, then risk teams can prevent future purchases on the same card before they're ever initiated.

Risk teams can even use their insights to quickly create, develop, and deploy customized risk-time rules that will alert on newly-identified fraud scenarios and patterns.

Unit21's transaction monitoring solution empowers teams to shift from simply detecting fraud to preventing it by allowing them to deploy rules that analyze transactions in real-time for immediate interdiction or review.

The challenges and limitations of real-time monitoring

Risk professionals acknowledge the challenges in preventing fraud. Yes, you can decline all the transactions and stop all the fraud, but how do you balance between safety and friction? That balance becomes even more sensitive when moving from batch to real-time payments, where consumers expect their funds to be processed instantly.

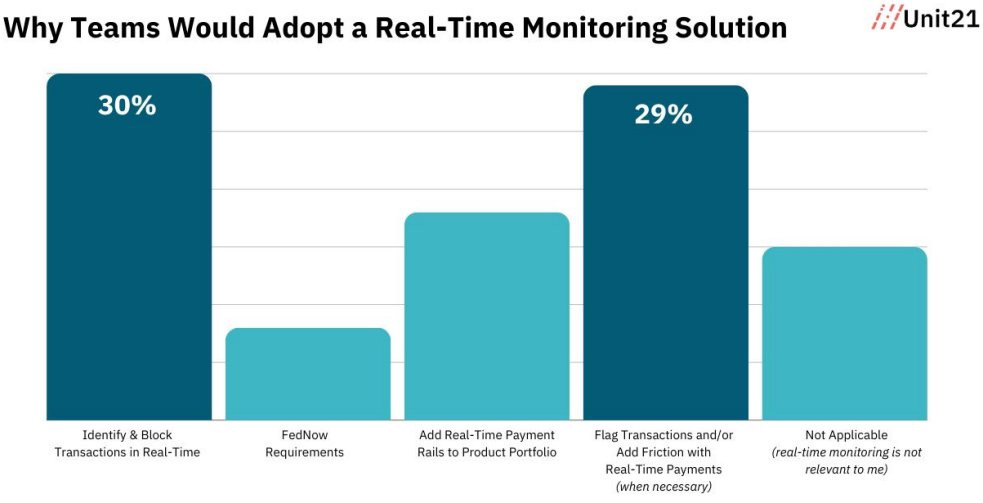
These are some of the biggest challenges that fraud & risk teams face with real-time payments:

- **Defining 'real time':** Real-time is never truly instant, and it's not universal across institutions. Since latency issues can lead to system errors that allow fraud to pass through unchecked, it's imperative that your organization clearly defines what it means by *real-time* and what portion of the authorization flow will be dedicated to fraud prevention.
- **Working within a short window:** Real-time monitoring gives risk professionals a very small window to analyze and action a case. Risk teams need to ensure they're managing that time as effectively as possible. Every millisecond is valuable and should be accounted for.
- **Managing data speed and volume:** Pushing transaction speeds to their limit comes with significant data management challenges—especially when you're also handling large transaction volumes.
- **Maintaining data quality:** Real-time processing leaves very little time to identify errors in data quality, making it more important than ever to ensure the integrity of your data. Even a small error can have a butterfly effect on all proceeding decisions and actions.
- **Managing Operational Risk:** Real-time monitoring means fraud teams must work 24/7/365, for FIs that translates into more personnel, investing in training, and much higher expenses for the fraud program.
- **Failing to have an action plan:** Many teams dive head first into fraud prevention, collecting as many signals as possible, often without thinking about how that data will actually be used to detect and prevent fraud. Rather than being 'data rich and information poor,' risk teams need to define the data and risk signals that are important to them, and then effectively leverage that information to mitigate fraud.

Unit21 takes care of these worries for you. Make decisions confidently and swiftly with low-latency processing (250 milliseconds!), and let us handle data speeds, volume, and quality for you.

Why teams invest in real-time monitoring solutions

Despite the challenges they face, fraud fighters understand the power of being able to identify, flag, and block transactions in real-time.



Data Source: *State of Fraud and AML Report Volume 2, Unit21*

Very few of our 2023 State of Fraud Report respondents were planning to use real-time monitoring to meet FedNow requirements or implement their first real-time payment rail. The majority of risk professionals leveraging real-time monitoring solutions are already battling real-time payment fraud, and understand that it's an invaluable tool for not only stopping fraud, but also hindering fraudsters by adding friction where it'll hurt them most.

Simply put, most risk professionals understand that real-time monitoring is an essential element of detecting and preventing real-time payment fraud, empowering them to prevent fraud losses and proactively stop fraud from occurring.

But risk professionals also understand that real-time monitoring isn't just for real-time payments. It can also be used to alert on other rapid transaction fraud like credit card payment and credit card testing fraud. Teams can then use this information to quickly react to future transactions by the same user or to quickly deploy rules to detect and prevent the new threat.

6 scenarios where real-time monitoring is necessary

Real-time monitoring can cut the time to action by making automatic decisions and alerting on suspicious activity in real-time, as the fraud is happening. In some cases, this can empower teams to actually interdict transactions, preventing fraud before it happens. In other cases, it allows teams to be alerted immediately after a successful fraudulent attempt, allowing teams to recover the funds and block further transactions by the culprit.

Real-time monitoring is ideally suited to detect and prevent fraud in a variety of fast-payment fraud scenarios. Below, we cover a handful of the most important applications.

1 Authorized Push Payment (APP) Fraud

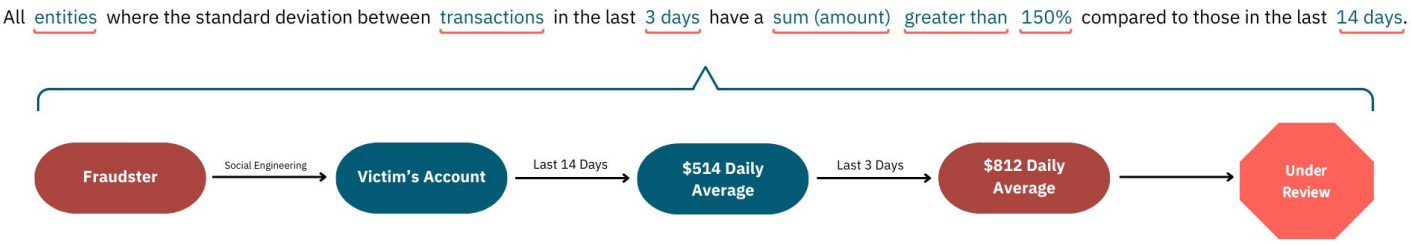
Real-time payments are prime targets for Authorized Push Payment fraud. After fraudsters convince their victims to authorize a transfer, the funds are sent and settled immediately, giving victims—and fraud prevention teams—little recourse for recovering funds. And since the payment was authorized, there is little proof the transaction was fraudulent at all.

Real-time monitoring solutions check for transaction anomalies in real-time to flag a transaction as suspicious. They do this by leveraging a variety of signals, including transaction values, transaction volumes, recipient location, device type, and the user's IP address. With enough signals available, risk teams can develop rules that automatically block transactions that could be APP scams.

Example Rule
Look for anomalies from a customer's typical behavior patterns using a historical deviation model.

- All entities where the standard deviation between transactions in the last 3 days have a sum (amount) greater than 150% compared to those in the last 14 days.

Example Rule for APP (Authorized Push Payment) Fraud



2 Account Takeover (ATO) Fraud

Account takeover fraudsters know they have a short window of time to operate before an account holder or financial institution (FI) realizes the account is compromised. Typically, they act quickly to steal information and drain accounts before they're found out.

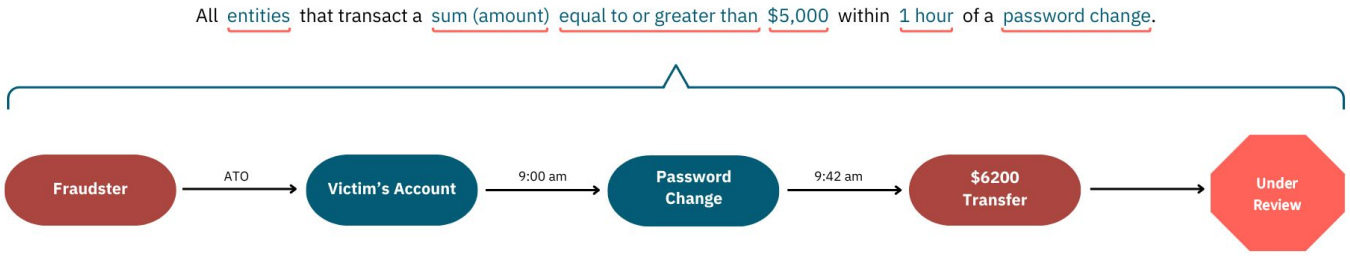
This means risk teams need to be able to act quickly to stop the account takeover itself, or the fraud that's sure to follow. With the right signals at their disposal, risk teams can use real-time monitoring to identify when account takeover has occurred, is in progress, or is likely to occur.

Real-time monitoring tools can flag account changes that may be indicative of account takeover, watching for changes to passwords, contact details, mailing addresses, and more. They can also look for anomalies in IP addresses, device types, and geographic locations that may signal account takeover has occurred.

Example Rule
Look for high value transactions that occur shortly after a major account change, such as a change to the password, email address, or mailing address.

- All entities that transact a sum (amount) equal to or greater than $5000 within 1 hour of a password change.

Example Rule for ATO (Account Takeover) Fraud



3 New Account Fraud

Since real-time payments can process transactions that are irreversible, new account fraud (often using fake and synthetic accounts) poses a much more imminent threat on RTP rails.

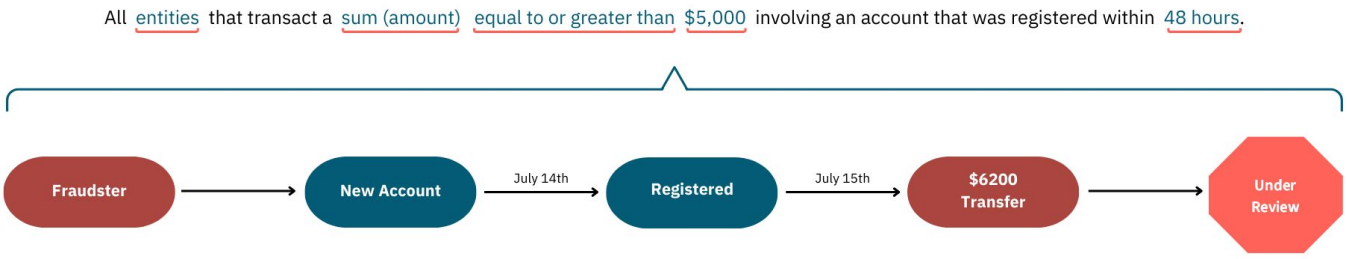
With no historical transaction or user behavior data to use as a baseline, real-time monitoring systems have little information to make a decision on these cases. Fortunately, real-time monitoring solutions can screen users against sanctions lists, deny lists, and other watchlists to identify potentially suspicious transactions.

Risk teams should also establish rules that monitor transactions from new accounts, setting greater limitations on new customers and watching for common risk signals.

Example Rule
Screen new users against watchlists to ensure they aren't sanctioned or deny-listed. Create rules that look for users that have registered recently, monitoring for abnormally high values or volumes of transactions from these users.

- All entities that transact a sum (amount) equal to or greater than $5000 involving an account that was registered within 48 hours.

Example Rule for New Account Fraud



4 Stolen or Compromised Cards

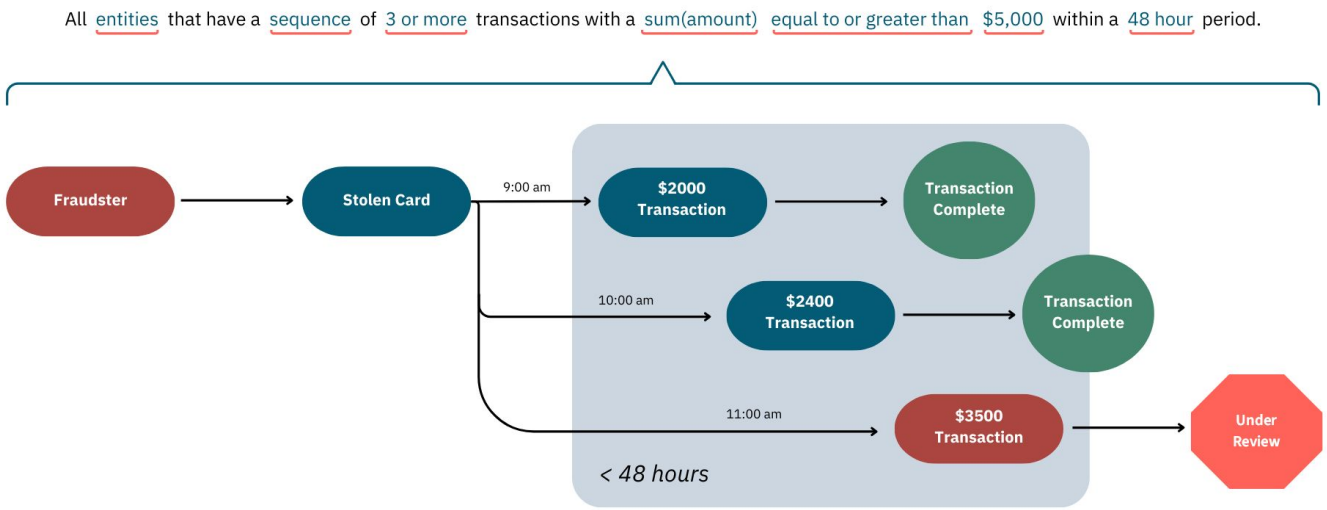
Stolen and compromised cards (or card credentials) are a real problem for risk teams, and that's only exacerbated by real-time payment options. Since real-time payments are irreversible, transactions made using stolen or compromised cards are extremely hard to reconcile.

Real-time transaction monitoring can be used to identify potential fraud. If a card shows abnormal behavior with large transaction values or volumes, that could be an indication of this type of fraud. Teams that can monitor for these transactions in real-time can drastically limit the number of successful transactions that fraudsters can complete.

Example Rule
Look for a sequence of transactions totalling a high value within a short span of time.

- All entities that have a sequence of 3 or more transactions with a sum(amount) equal to or greater than $5000 within a 48 hour period.

Example Rule for Stolen or Compromised Cards



5 Card Testing

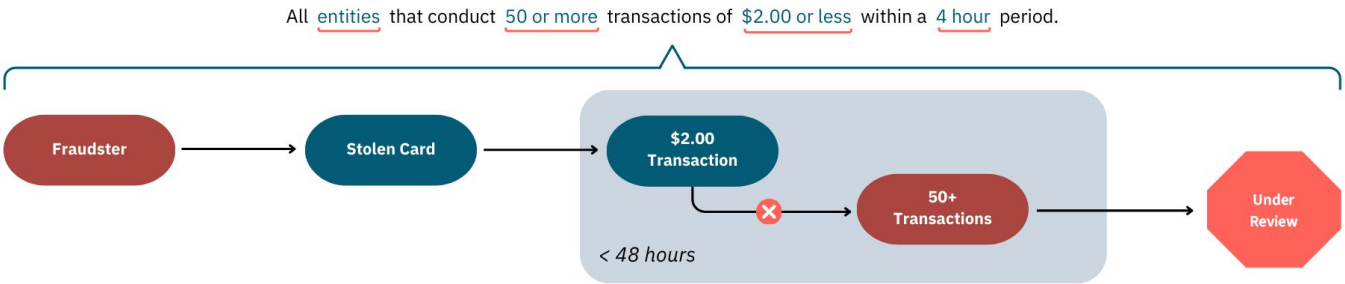
Before really letting loose, many fraudsters test stolen card credentials to make sure they'll be able to successfully complete transactions or transfers. Once they know the card credentials they have will work, they'll begin committing fraud in earnest, making larger purchases.

Since card testing always precipitates further fraud, if teams can stop the fraudster during this card testing process, teams can significantly reduce the fraud losses that would follow. Real-time monitoring can be used to detect card testing fraud, allowing teams to block the fraudster before fraud losses pile up.

Example Rule
Look for entities conducting a high volume of low value transactions in a very short period of time.

- All entities that conduct 50 or more transactions of $2.00 or less within a 4 hour period.

Example Rule for Card Testing Fraud



6 BIN Attack

Fraudsters using BIN attacks don't waste time social engineering their victims or phishing for personal information. They cut to the chase and try to force access to a victim's credit card using brute force computing that guesses all potential variations of their card number, expiration date, and customer verification value.

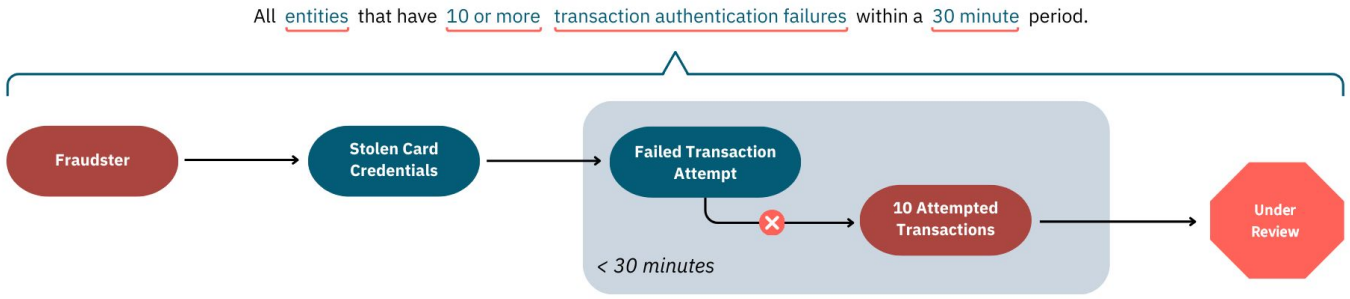
BIN attacks themselves are attempts at card payment fraud. If teams can get real-time alerts on BIN attacks, they can potentially step in before the card payment fraud that typically follows this type of fraud occurs. But BIN attacks—unlike some other types of fraud—aren't tied so strictly to a single card or account. Instead, risk teams will need to monitor activity on a program level, looking for how many cards on their platform are experiencing the same activity.

Example Rule

BIN attack rules typically operate on a program level. You can monitor for BIN attacks effectively within a queue within Unit21. If you see a high volume of alerts in the queue over a short period of time that are coming from the same merchant, IP address or same transaction amount, you can investigate further for possible BIN attacks.

- All transactions that are declined with invalid card, card not found or CVV errors within a 30 minute

Example Rule for Bin Attacks



Real-time monitoring considerations & best practices

Real-time monitoring solutions are demanding, coming with a lot of challenges in terms of implementation and management. Fortunately, there are ways to make this transition easier on yourself and to increase your chances of success.

Below, we cover some of the best practices to follow (and most important things to consider) when it comes to real-time monitoring.

Fast-track trusted customers

A customer attempts to make a legitimate purchase, and they're blocked by a false positive alert for fraud. How do you ensure that this customer doesn't get wrongfully blocked again?

Risk teams can use white labeling to easily keep track of low-risk, trustworthy individuals that have previously been falsely denied service, ensuring they get a seamless customer experience moving forward.

Allow lists can also drastically reduce the load on real-time monitoring processes and systems by reducing the amount of unnecessary alerts being processed through your system. In turn, this mitigates an overload or backlog of alerts. It's an essential tool for effectively managing your real-time monitoring workload without adding undue risk.

See how you can set up allow lists to reduce your false positives with Unit21's RTM tool.

Consolidated data and single data visualization

Look beyond just the transaction itself, instead using all the data at your fingertips to create a holistic view of the customer and their behavior.

The more information you can feed into your real-time monitoring system, the more effectively, accurately, and efficiently it will be at identifying, alerting on, and potentially interdicting fraudulent transactions.

Unit21 integrates seamlessly with your third-party risk infrastructure to consolidate and unify data, empower faster, deeper, and more accurate analysis (without costing you more time). Investigators can get to the bottom of a case much faster and risk teams can confidently rely on their system to alert—or act—suspicious activity it detects in real-time.

With enhanced user data available alongside transaction data, investigators can identify anomalies in user characteristics that would otherwise go unnoticed, such as a risky IP address or a login from an abnormal device type.

Low-latency

When you're operating in a window that's 20 seconds or less, every millisecond counts. Having a system with low-latency is not only advantageous, it's vital.

High-latency can lead to delays and errors, which ultimately translates into higher fraud losses. If the system can't make a determination in time, it will either allow fraud to pass through undetected or turn away legitimate customers because it can't review their transaction in time. Either way, dissatisfied customers will leave to find a solution that doesn't wrongfully bar them from transacting and fraudsters will flock to take advantage of your security failure.

Unit21 knows that the slightest hiccup can have significant and long-lasting effects. That's why our real-time monitoring solution processes decisions within 250 milliseconds!

Cross-reference deny lists, sanction lists, and other watchlists

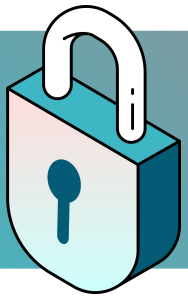
Avoiding business with individuals and entities on sanctions lists isn't just a matter of fraud prevention, it's a matter of compliance. Failure to adequately screen new and existing customers against sanctions lists can lead to fines and penalties, as well as expose organizations to fraud losses.

Real-time monitoring empowers teams to cross-reference customer data against deny lists, sanctions, and other watchlists that could indicate whether an individual or entity is high-risk. When used effectively, these solutions can flag high-risk individuals for further review or even automatically block them from accessing your platform, inhibiting them from committing fraud.

Consider the operational costs and workload

Real-time monitoring solutions typically require a larger lift than non-real-time alternatives. They have to be operational around the clock with consistent low-latency, and this comes with additional financial and operational cost, increasing maintenance and engineering requirements significantly.

But that doesn't have to be the case. Unit21 knows that real-time monitoring can't wait, that's we have a seamless integration—your real-time monitoring solution can be operational with a single day of operational work. And our no-code solution means you don't have to commit engineering resources down the road; instead, you can build high-performing real-time monitoring rules that allow you to not only detect—but actually prevent—fraud.



Set up Real-Time Monitoring in just one day while strengthening your security. See how.

Save engineering resources with a no-code solution

One of the biggest hurdles with real-time monitoring is the time and engineering resources needed to implement a new rule. All of which takes time, money, and staff away from other tasks.

A no-code solution drastically reduces the engineering resources—and time— needed to get a new fraud prevention rule operational. This shortens the reaction time significantly, allowing rules to be created in minutes rather than weeks or months. Teams can then pivot quickly and nimbly to address new and evolving fraud threats.

Develop defined, targeted real-time rules

Before you set up rules that are going to add friction to the customer experience, you need to understand the impacted population and the expected fraud capture rate. You can't just establish rules with no understanding of how they'll impact your customers, or you'll end up with a lot of false positives—and just as many upset customers.

The more information you have on your customers, the more you can understand the fraud that's occurring and refine your rules to target that fraud specifically. Real-time monitoring empowers teams to create targeted rules that have low false positive rates, keeping customers happy.

Unit21 for Real-Time Monitoring

Unit21

Here at Unit21, we believe the more data you have, the more equipped you are to do your job. But having data isn't enough, it needs to be accessible and understandable so that risk teams and systems can draw meaningful conclusions from the information on hand.

And quite frankly, if data isn't acted on quickly, it can start to lose its value. We help teams collect data, organize that data into a visualization that teams can draw meaningful insights from, and empower risk teams to make faster, more informed decisions.

It's all about cutting through the clutter to find the signals that matter most to you.

First & third party fraud

Fraud can be committed by anyone, ranging from a malicious account takeover from a third party to friendly fraud committed by the account holder themselves. Risk teams need to be prepared to address everything in between.

Fortunately, Unit21 has out-of-the-box, real-time rules for some of the most common 1st and 3rd party fraud scenarios. But you still have the flexibility to refine and customize these pre-built options or create your own entirely from scratch.

Key features & capabilities

Here at Unit21, we know you don't want to be spending time engineering new rules and developing your risk infrastructure. That's why we handle that for you, instead empowering you with tools that allow you to build fraud detection and prevention rules and systems quickly and seamlessly. This way, you can focus on actually preventing fraud.

Here are some key features that make Unit21 stand out as an ideal real-time monitoring solution for anti-fraud:

- **Reduce Fraud Losses:** Real-time monitoring allows risk teams to automatically approve or block transactions within 250 milliseconds, slashing fraud losses and offering a seamless user experience.
- **Automatically Generate Alerts:** Alert generation and prioritization is fully automated, so teams can focus on actually investigating cases and updating strategies. Real-time monitoring helps risk teams shorten the time to action by ensuring suspicious activity doesn't go unnoticed (or get lost in the clutter).
- **Find the Signal in the Noise:** For teams with a high-volume of alerts, it can be challenging to identify the data that matters most. We not only provide you with a wealth of information to help you decision cases, but we help you identify the factors that actually matter most for mitigating risk.
- **Create and Implement Rules in Minutes, Not Months:** Being able to create fraud detection and prevention rules in a no-code environment empowers teams to implement rules rapidly and on-demand, without requiring any engineering resources to make it happen.
- **Reduce False Positives:** With the ability to customize rules to fit your audience and ecosystem, you're able to refine rules and mitigate false positives—without letting more fraud pass through your system.

Our risk infrastructure offers real-time monitoring solutions alongside the rest of your risk operation, so you have all your risk management data in a single place. Paired with our customizable rules engine, risk teams can automate processes that block, flag, and hold transactions to streamline risk management operations.

The Future of Real-Time Payments and Monitoring: Concluding Thoughts

Unit21

Global real-time payment adoption speaks for itself—real-time payments are here to stay.

While the U.S. certainly lags behind other countries, the recent FedNow push has been fueling RTP network adoption, whether that be with the FedNow or The Clearing House's RTP. With only 1.2% of all payments in the U.S. being real-time in 2022 and a total electronic payment share of 81%, the U.S. market is primed for real-time payment growth in the coming years.

As payments increasingly shift to real-time payment rails, fraudsters will follow, shifting their attacks to real-time payment rails that give them access to transactions that are **instant** and **irrevocable**. The tactic of choice for RTP rails seems to be APP fraud, as authorized payments raise less suspicion and give the victim's less recourse for recovery.

With payments traveling virtually instantly, real-time monitoring is no longer optional—it's essential. Without it, it's impossible to detect and prevent fraud on an RTP rail. While some risk teams have been using RTM for real-time fraud applications other than RTP, there is no question that monitoring real-time payments is impossible without an effective RTM solution.

Risk management teams looking to provide their organizations and customers with adequate safety and security will need a real-time monitoring system that:

- Fast-tracks trusted customers using allow lists
- Consolidates data into a unified view
- Scores and prioritizes alerts so you can cut the signal from the noise
- Operates on low-latency with no hiccups so you never miss an instance of fraud

Unit21's real-time monitoring infrastructure is designed to offer proactive protection against real-time fraud threats, analyzing transactions, behaviors, and networks for anomalies. With one of the lowest-latencies on the market (250 milliseconds!), you can be confident that our RTM will be able to work quickly to accurately approve or block transactions.

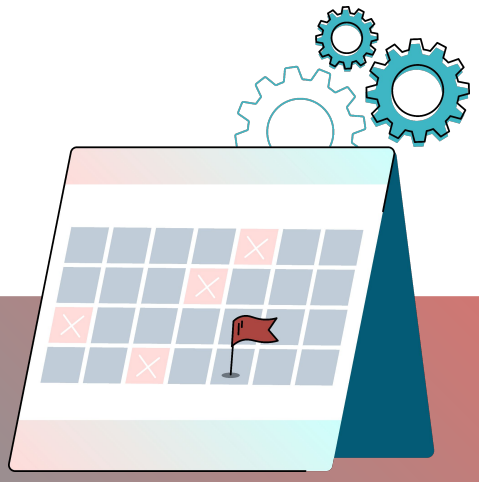
We don't just make monitoring transactions fast either, we also know integration and setup are a major hassle that can set your risk team back on their deadline. With Unit21, you can be operational within a single day.

Get pre-built, out-of-the-box rules for common real-time fraud scenarios so you can have rules set-up right away. That being said, our rules are fully customizable, so you can fine-tune existing rules for better results or build your own rules entirely from scratch. And with no-code required, teams can create and deploy new rules in minutes (not days or weeks!) with no engineering required.

In 2023, we:

- Monitored 4.05 billion events
- Monitored $2.77 trillion in transactions
- Detected $4.3 billion in fraud
- Handled over 28K SARs
- Latencies of <250 ms

Unit21



Schedule a demo

with us today to learn how Unit21's real-time monitoring offering could help your team detect and prevent fraud, stem fraud losses, and keep your platform—and customers—safe from fraud.