Unit21

WHITEPAPER

The Scam-demic

How FIs & Fintechs Can Fight Back Against the Latest Scam Threats

TABLE OF CONTENTS

What's Inside

Introduction

The prevalence of scams and the losses associated with them are increasing at an alarming rate.

The adoption of AI, the play on one's emotions, and more sophisticated technology are all contributing to the rise in scams. Banks and credit unions are struggling to prevent and detect these scams, often becoming aware of them after being reported by customers.

This whitepaper examines the evolution of scams, why scams are a unique threat, regulatory gaps that exist today, and Unit21's solution to combat this growing trend.

The New Frontier in Fraud

Fraud is a tale as old as time. The first fraud case has been dated back to 300 BC between two Greek sea merchants who essentially committed insurance fraud. Since then, fraud has continued to morph and change as technology advances and new payment rails are developed. People such as Frank Abengale, famous for check fraud, and Bernie Madoff, known for his Ponzi scheme, have become household names when it comes to fraud. Scams are just the latest evolution in payment fraud.

Scams are a unique subset of fraud. They are specific schemes designed to deceive individuals for financial gain. They focus on exploiting trust through social engineering, manipulation, or misrepresentation. Fraud, on the other hand, is a broader legal term for deliberate deception intended to secure an unfair or unlawful gain or to deceive a victim of their rights. It's important to note that while all scams can be considered fraud, not all frauds are scams.

Many different types of scams are prevalent today. Imposter scams happen when a fraudster pretends to be someone else to persuade you to do something. Online shopping scams include buying products or services that don't exist or overcharging you for

1 "5 of the most remarkable instances in the history of fraud," Experian, https://www.experian.co.uk/blogs/latest-thinking/fraud-prevention/5-of-the-most-remarkable-instances-in-the-history-of-fraud/, September 2015.

products. Prizes and lottery scams promise money or prizes but instead focus on advanced payments to cover "fees". Investment scams trick people into sending money to a fraudster instead of an investment. Romance scams exploit trust by convincing someone they are in a relationship before that person asks for money. Work-from-home scams are becoming more prevalent, using victims to be money mules disguised as actual employees. And the list goes on.

What's interesting about scams is that other fraud verticals may be the result of a scam. Fraud may ultimately result in something such as an account takeover (ATO), but it was initially a scam that allowed the fraudster to retrieve the login credentials. This makes it difficult to pinpoint how much money is lost to scams annually, as financial institutions and others may report scams as another fraud type.

What is known is that scam losses are increasing rapidly. According to the Global State of Scams Report 2024, scammers stole $1.03 trillion globally over one year.[2] The Federal Trade Commission reported that consumers lost more money to investment scams than any other category in 2023. The second-highest reported loss came from imposter scams.[3] And, the United States is the most scammed country in the world with the United Kingdom coming in second.[4]

The increase in the number of scams, the various scam types, and the losses associated with them make it difficult to keep the public aware and almost impossible to prevent and detect. Fraudsters are changing tactics quickly and the use of Artificial Intelligence makes these scams more realistic than ever before. And with every new payment rail or fraud type that enters the market, regulations are always lagging, trying to keep up.

Scammers stole $1.03 trillion globally over one year.

2 "Global State of Fraud Report 2024", Global Anti-Scam Alliance (GASA), www.gasa.org
3 "As Nationwide Fraud Losses Top $10 Billion in 2023, FTC Steps Up Efforts to Protect the Public", February 9, 2024, https://www.ftc.gov/news-events/news/press-releases/2024/02/nationwide-fraud-losses-top-10-billion-2023-ftc-steps-efforts-protect-public
4 "Infographic: The U.S. and Scams", February 29, 2024. https://blog.usalliance.org/infographic-the-u-s-and-scams

The Evolution of Scams

Scams began before the 1900s using the art of deception. Con artists employed simple tricks to exploit trust in personal interactions. In the early 19th century Gregor MacGregor, a Scottish soldier, sold land to investors in a country that didn't exist. He used marketing efforts and lies to attract investors, many of whom lost their life fortunes.

The introduction of the telephone brought in a rise in phone scams. Without things like caller ID, people were trusting when answering the phone, assuming that the person on the other end was who they claimed to be. Scammers impersonated banks, insurance agencies, and the like to gain personal information they could use to steal money. The use of lottery schemes via telephone and mail was also popular. "Winners" were asked to send in a processing fee to claim their prize, unaware that the check they received, or the prize promised was fake.

In the 1990s email scams came on the scene, bringing attention to the infamous Nigerian Prince scam, and marking the dawn of online fraud. Victims received an email from this "prince" claiming to need help getting a huge amount of money out of their country. The victim would be asked to provide either bank account details or money to pay for fees. In exchange for their willingness to help, they would receive a large sum of money. Of course, once they paid the fees or provided their bank account details, the money never came. And some victims' accounts were drained before they realized it was a scam.

The 2000s ushered in the era of digital deception. Phishing attacks became widespread, with scammers impersonating banks and companies to steal personal information. Links were used to either capture online credentials or place harmful malware on computers, all to drain funds and steal personally identifiable information (PII) to use for illicit gain. Both the Nigerian Prince emails and phishing emails were wrought with spelling and grammatical errors. Educational efforts began to help spot the red flags and keep consumers and businesses safe.

64%

of **banks** say scams are on the rise

33%

of **CUs** report scams surging by 50-100%

compared to the prior year

#1

most time-consuming fraud for **fintechs**

Source: Insights from the 3rd Annual State of Fraud and AML Report

As smartphones became the norm, the mobile revolution gave way to P2P (Person-to-person) payments, making it easier than ever before to send money to family and friends. However, the speed of payments made it ripe for fraudsters to exploit the immediacy of transactions and use social media to target potential victims. Mobile payment apps led to new scams and new vectors for fraud.

Today, consumers and businesses are facing more sophisticated scams. The use of AI makes it virtually impossible to detect more sophisticated scams, eliminating the red flags of common grammatical errors in scams of the past. Phishing scams look more realistic, forcing everyone to always be on the defense, scrutinizing every email and text to determine its authenticity. Romance scams are taking off, with scammers impersonating other genders and ages to attract potential victims. After building rapport, the scammer then leads the victim to believe their loved one needs money or, in a new twist, convinces them to join them in a seemingly lucrative investment opportunity.

Authorized Push Payments (APP) have made it easier and faster to pay for goods and services. With that ability comes APP scams. Fraudsters convince people to authorize a payment and then there's little to no recourse once it's been sent. The person has been manipulated but because they were the ones that initiated the payment, the onus is on them. Oftentimes they are buying goods or services that don't exist, paying money to a "loved one" through a romance scam, or sending money to a supposed investment.

The use of AI makes it virtually impossible to detect more sophisticated scams, eliminating the red flags of common grammatical errors in scams of the past.

Why Scams Are a Unique Threat

So, what is it about scams that make them so unique to other fraud vectors? Scams are the evolution of fraud, a culmination of the different vectors all playing on different aspects from believing the authenticity of a payment, to the trust given to the impersonator.

1 Exploitation of Trust

Human nature defaults to people being truthful. And although it's easy to believe the perception that only gullible people fall for scams, that's far from the truth. Someone doesn't have to be a vulnerable person, but rather, just have a moment of vulnerability. And, at the end of the day, people want to be able to trust one another.

Scammers use social engineering and manipulation to gain trust before breaking it. With romance frauds, scammers prey on the victim's need or want to be loved. These scams usually last longer, taking the time to build that rapport and gain their victim's trust, making them believe they are in a legitimate relationship.

With scams such as sextortion, the victim believes they are texting or chatting with the person whose picture they see. Oftentimes it is men manipulated into thinking they are conversing with a young, attractive female. The scammer often sends a nude photo first, creating a component of trust and making it a more believable scam. Then they coerce their targets into sending a photo in return. Regardless, it still comes down to trust and believing that they know who is on the other side of the conversation.

2 Fast-Moving Funds

The days of working the float when mailing checks are in the past. Businesses and consumers alike are pushing for faster payment methods. Faster payments allow businesses to wait on payables, managing their own liquidity. Consumers can pay bills and other individuals quickly and easily. The adoption of Real-Time Payments (RTP) is exponential. Funds are moving quickly and often, payments are irreversible, making them prime targets for fraudsters.

It also makes recovery nearly impossible once fraud is discovered. When you speed up the processing of payments, it gives financial institutions less time to detect and prevent fraud, let alone stop it. Even with things like the remittance transfer rule, allowing consumers to cancel wires within 30 minutes of sending, it doesn't help when the consumer was the one who initiated the payment while being manipulated by a scam. Plus, most scammers prefer the use of faster payments and APPs instead of traditional methods such as check, wire, or ACH. While those payment rails are still used in scams, the use of faster payments is more appealing to fraudsters, allowing them to get away with the money before any recourse can be made.

3 High-Tech Scammers

In the world of scams, fraudsters love to make what's old, new again. Scammers leverage new technology to evolve the tried-and-true scams that have been the most effective, making them even more sinister. Using things like AI and spoofing makes it incredibly difficult for individuals to discern what's real and what's fake.

As mentioned above, phishing scams were wrought with grammatical errors and were easily detectable. ChatGPT and other AI chatbots allow scammers to improve the text to near-perfect English, reducing the number of red flags.

AI has also made it far easier to scale an attack. Instead of running a single scam on a single victim at a time, AI and advanced technology allows scammers to run the same scam automatically on thousands of victims at once, increasing their chance of a payout.

Sometimes victims get a sense that they may be involved in a scam and will ask the other person to do something like a peace sign or a thumbs up to determine legitimacy. Today, criminals can put the photos of whatever model they are using into an AI system, have the system portray whatever the victim has asked for, and provide the needed "evidence" to convince the victim that the person is "real".

In the case of sextortion, even if the victim doesn't send a return photo, the criminal can take pictures from their public Instagram or Facebook account, run it through an app like Nudify or Clothes Off, and remove the clothes and use that fake photo to blackmail their target.

Scammers now have access to deep-fake technology that allows them to not only imitate someone's voice, but their likeness via video. Things like the infamous grandparent scams where a scammer calls imitating a grandchild in need of money are now more likely to succeed when sounding just like their loved one.

The Regulatory Gap: Playing Catch-Up

With all fraud, scams have become a global problem. Governments everywhere are trying to crack down on scammers and implement rules and regulations to stop scams before money is lost. In addition, the scams can be perpetrated anywhere, making it even more difficult to prosecute in countries where there is no jurisdiction. Even if the fraudsters can be pinpointed, there's little that can be done.

As scams and scam losses continue to increase, regulatory agencies have struggled to keep up. There has not been clear guidance on what constitutes proper safeguards, yet institutions that fail to provide such safeguards can be held liable. In October 2024, the Payment Systems Regulator, which regulates the payment systems in the UK, created rules applying to payments service providers requiring them to reimburse customers who become victims of APP fraud. The rules outline the scenarios in which reimbursement is warranted and states what payments do not fall into this category.[5]

Banks in the UK also have the authority to put a four-day hold on suspicious transactions. Banks should only use this when they have reasonable grounds to suspect fraud, in an effort not to disrupt payments. However, this gives institutions additional time to investigate potential fraud.[6]

The Albanese Government created the National Anti-Scam Centre, which is a partnership between the government, law enforcement, and the private sector. In November 2024, the government introduced into Parliament the Scams Prevention Framework, which would require banks, social media platforms, and telecommunications companies to take reasonable steps to detect, disrupt, and report scams or face hefty fines. This legislation also requires there to be a coordinated intelligence-sharing ecosystem.[7]

Both the UK and Australia have developed a Confirmation of Payee (CoP) designed to allow payees

5 "APP fraud reimbursement protections," Payment Systems Regulator website, https://www.psr.org.uk/information-for-consumers/app-fraud-reimbursement-protections/.
6 "Banks to put four-day hold on suspicious payments", BBC, https://www.bbc.com/news/articles/cn7yel28rx6o, October 3, 2024.
7 "Albanese Government introduces landmark Scams Prevention Framework," Ministers Treasury Portfolio, https://ministers.treasury.gov.au/ministers/stephen-jones-2022/media-releases/albanese-government-introduces-landmark-scams, November 7, 2024.

The APP regulation may seem to be a proactive approach, but critics claim that although consumers are no longer taking the burden, the brunt is felt by the financial institutions and still doesn't get to the heart of the problem. It's a reactive solution, allowing scammers to still get away with stolen funds.

to verify if an account name matches the name of the recipient before authorizing a payment. The decentralized banking system in the United States would make creating such a platform difficult. Plus, fraudsters have already figured out how to create account names similar enough to get through the cracks of these platforms.

The passage of the APP law in the UK and the four-day hold, plus the partnership of the National Anti-Scam Centre in Australia has sparked talk amongst regulators in other countries. Is this the direction others should go in to safeguard consumers? The APP regulation may seem to be a proactive approach, but critics claim that although consumers are no longer taking the burden, the brunt is felt by the financial institutions and still doesn't get to the heart of the problem. It's a reactive solution, allowing scammers to still get away with stolen funds.

Reimbursements for scams are not currently mandated in the United States. Often, banks are reimbursing customers on a case-by-case basis. Financial institutions within the US are spending billions on anti-fraud measures. However, many are denying reimbursement claims from customers citing the Electronic Funds Act. That law does not explicitly state that banks must reimburse customers when the customer was tricked and authorizes the payment. There are specific instances where customers are covered under the Electronic Funds Act. For example, if someone were to hack their account and create a transfer that was not authorized.

In December, the Consumer Financial Protection Bureau (CFPB) filed a lawsuit against Early Warning Services and three major banks, alleging that they ignored complaints about scams within the Zelle platform, leading to losses totaling hundreds of millions of dollars. JPMorgan accused the CFPB of overreaching and trying to make banks liable for scammers. There are claims that Zelle has been slow to implement anti-fraud measures, including the closure of accounts associated with fraud.[8]

The partnership in Australia highlights the need for better communication between sectors. Today in the United States, financial companies that are not banks or credit unions are often not held to the same regulatory standards. Social media companies and government agencies are not sharing information and traditionally, social media platforms are not held liable for user or criminal behavior on their platform because that's another third party. What they are liable for is to build a safe product and build a product that has good privacy safeguards. Criminals often use the same images and videos repeatedly across platforms, yet they often go undetected. There are dangerous organizations that have public pages where information is shared on how to commit certain scams. It wasn't until recently that certain platforms have made concerted efforts to remove such pages.[9]

8 "Feds sue Zelle, alleging that nation's biggest banks failed to stop fraud," CBS News, https://www.cbsnews.com/news/zelle-fraud-chase-bank-of-america-wells-fargo-cfpb-payments/, December 20, 2024.
9 "Meta removes 1,600 Facebook groups linked to 'Yahoo Boys', launches campaign against sextortion", Vanguard, https://www.vanguardngr.com/2024/10/meta-removes-1600-facebook-groups-linked-to-yahoo-boys-launches-campaign-against-sextortion/, October 17, 2024.

Unit21 Solution

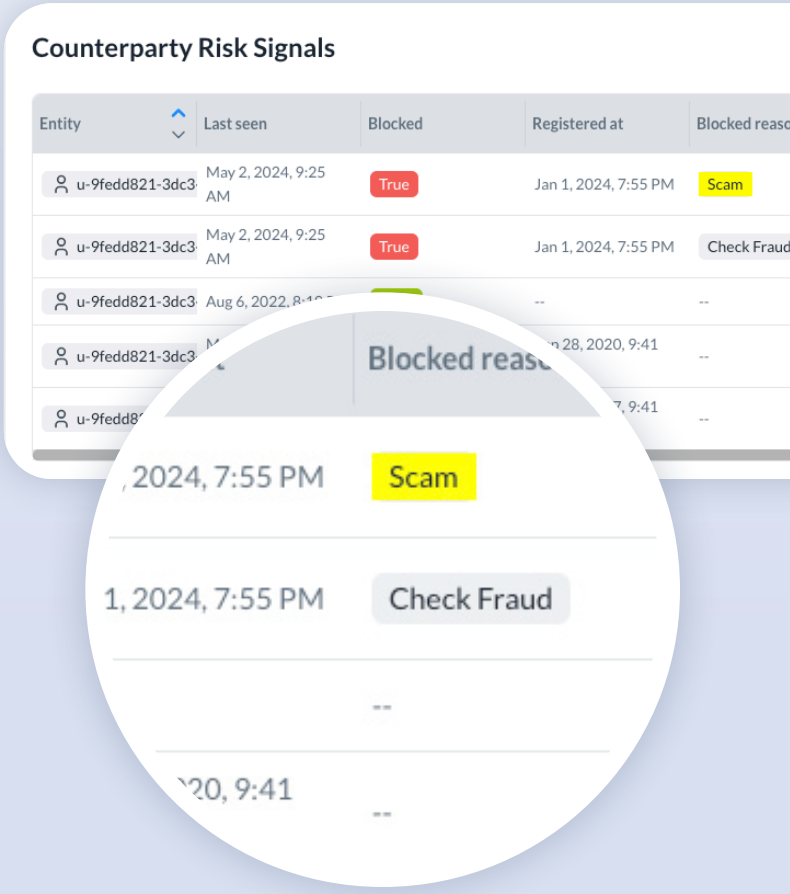
In response to the growing concern of scams, Unit21 has created a **comprehensive Scams solution** to look at scams from different angles, helping to alert financial institutions of suspicious or possible fraudulent activity.

Unit21's solution helps to prevent fraud, reduce costs, increase efficiency, and build customer trust and loyalty. The scams solution combines relentless innovation with proactive defense, empowering you to dominate the fight against scams.

Counterparty Risk

Counterparty Risk is a feature within Unit21's consortium that flags and alerts users about potential scam accounts before they can defraud others. This feature proactively notifies Unit21's customers if their customers are transacting with a known scammer, enhancing security without the user's immediate awareness.

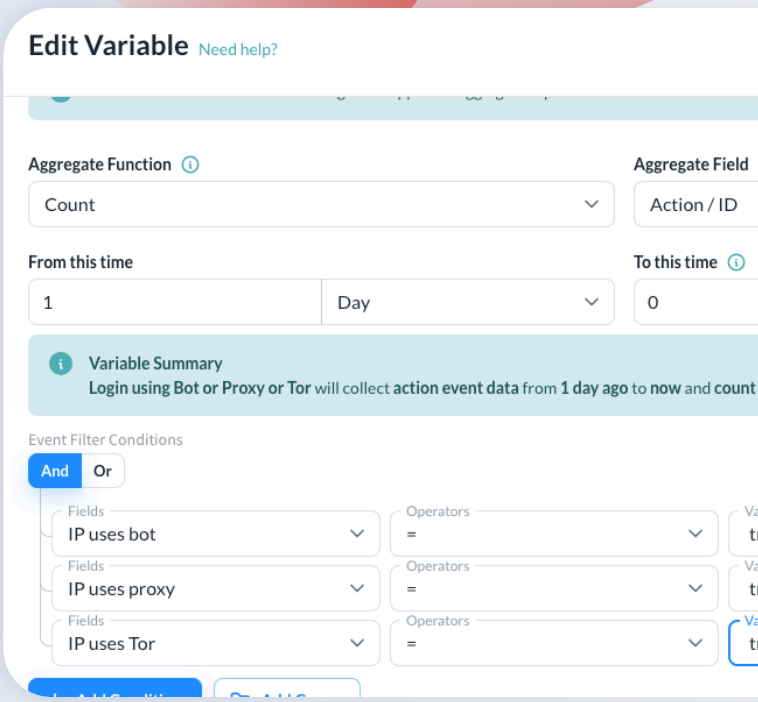
Consortium data can be used for identifying first-party fraud within a client's customer base but now can also be used to look at bank accounts that are known to be fraudulent payment destinations. Financial institutions are sharing information, and notifying one another when an account has been seen with positive behavior (payments coming in and no notices of fraud) and negative behavior (reported as fraud or scams). When sending customer payments, an institution can check the consortium to see if that payment destination has previously been associated with scams.



IP Data Enrichment

IP Data Enrichment enhances fraud detection by identifying IP addresses linked to bots, TOR networks, proxies, or VPNs. This powerful tool helps detect account takeover (ATO) by detecting masked login attempts and mitigates synthetic identity fraud by flagging suspicious account creation. It also curtails payment fraud and unauthorized transactions by recognizing high-risk IPs used for testing stolen credentials.

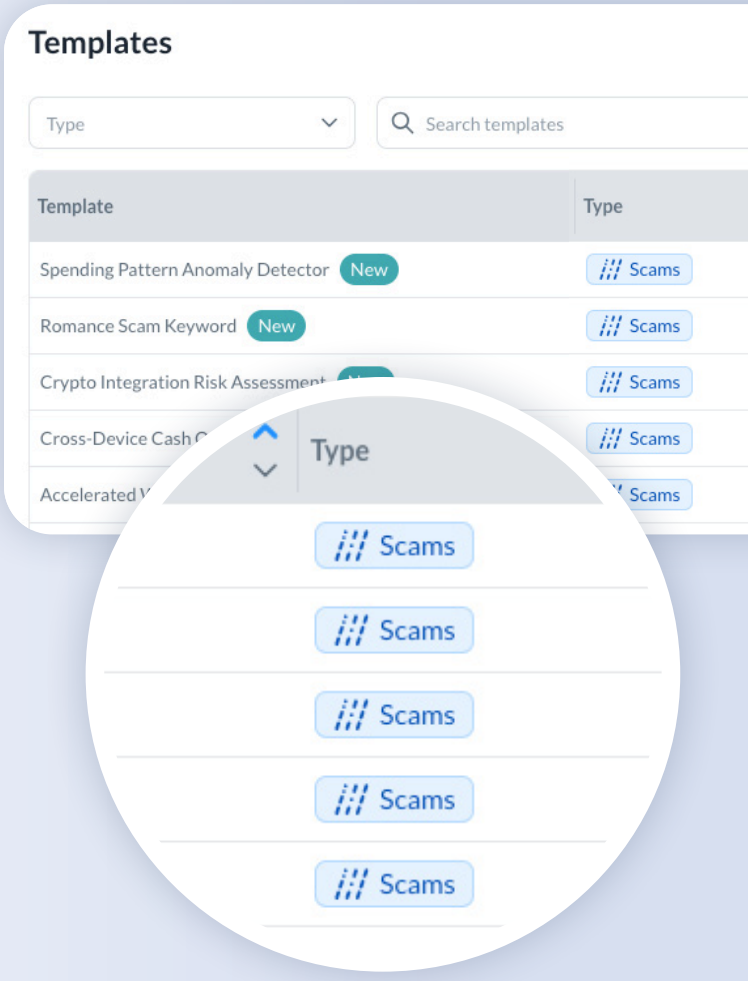
By integrating these insights into the rules engine, Unit21 empowers organizations to proactively catch scammers and stop scams before they escalate.



Scams Out-of-the-Box Rules

Scams OOTB Rules provide a powerful starting point for detecting and preventing fraud with minimal setup. These pre-built rules are designed to quickly integrate into your overall scam detection program, identifying suspicious behaviors such as unusual transaction volumes, flagged accounts, and rapid login attempts. While robust out of the box, they can be fully customized to align with your specific needs and evolving threats. By leveraging predefined criteria and real-time data, these rules empower organizations to rapidly respond to potential scams, reducing financial risk and enhancing security. Scams OOTB Rules offer the flexibility and adaptability needed to safeguard your operations in an ever-changing scam landscape.

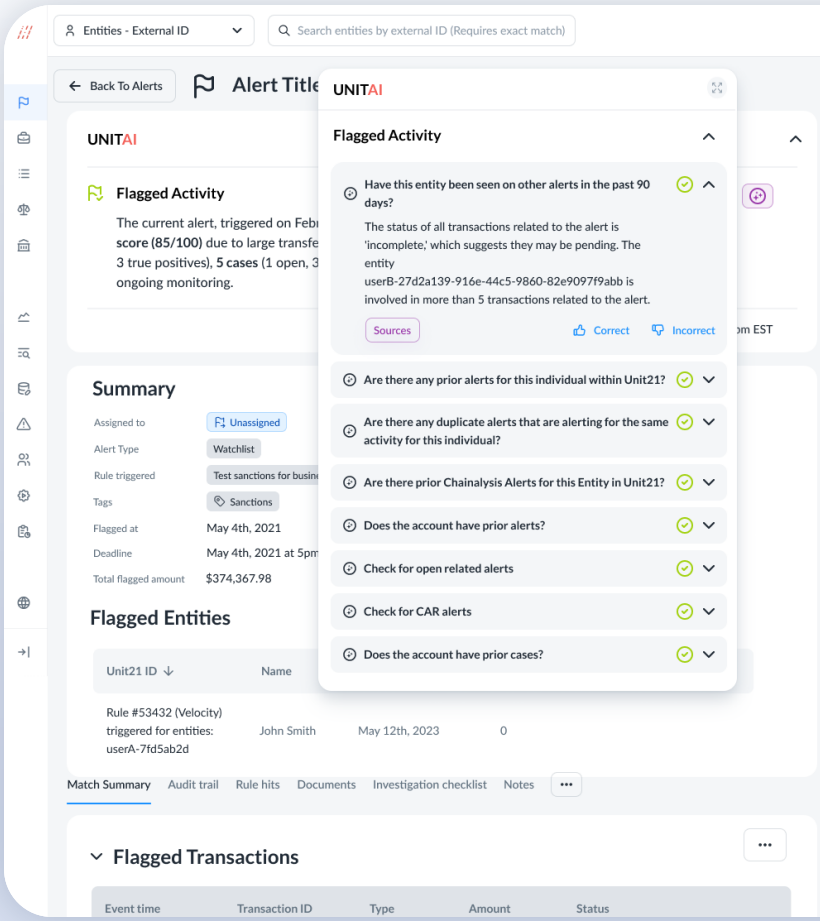
Scam tactics evolve rapidly, typically outpacing defenses. Using these OOTB templates allows FIs to quickly implement and turn around new rules, protecting customers and enhancing brand reputation.



AI Agent for Scams

Fraud investigations are cumbersome for analysts. It often requires looking at multiple platforms and searching for relevant data. The AI agent helps alleviate some of the manual work required by fraud investigators, especially when there are limited resources available. Manual work equals high operational costs. Using AI-driven tools helps to automate the fraud detection process.

The Unit21 AI Agent manifests itself as an AI-enabled checklist, evaluating key questions that help determine the legitimacy of transactions, such as anomalies in spending behavior, unusual transaction locations, and deviations from established user habits. This feature enhances fraud detection capabilities, enabling organizations to flag suspicious activities and prevent the negative consequences of the scams while lowering operational costs.



A Call to Arms

The surge in scams presents a formidable challenge. Scams are not only increasing in frequency but also can be costly and time-consuming for institutions to investigate and resolve. The pressure to reimburse victims further exacerbates the financial burden.

Institutions must employ proactive detection solutions to combat scams. Conduct internal fraud assessments to identify scam patterns and review current detection and prevention capabilities for effectiveness. Assess existing customer education programs and staff training needs. Institutions should also establish baseline metrics for measuring improvement in their detection capabilities.

The adoption of solutions like Unit21 can help stay ahead of threats and compliance mandates. Plus, information-sharing through consortium data gives you up-to-date information to stop a payment before it leaves.

Institutions must embrace a proactive and adaptable approach to combat fraud effectively. Taking proactive steps, investing in new technology, and fostering collaboration, all play a vital role in safeguarding against scams.