Confidence in Risk and Compliance: Modernizing Fraud and AML Management

Give your risk and compliance team the perfect balance of automation and control in managing operations

www.unit21.ai

Unit21

Contents

Overview

Fraud and money laundering continue to increase in scale, speed and sophistication — threatening the revenue and growth of financial teams. This ebook outlines:

- The alarming rate at which bad actors are tapping into new outlets for fraud and money laundering, and the need for a more robust defense.
- How organizations can benefit from an integrated approach to fraud and AML (Anti-Money Laundering) to gain more visibility and address their shared goals.
- How to future-proof teams by balancing automation and control, and putting Risk and Compliance technology in the hands of practitioners themselves; not engineering.

The ebook also showcases how two financial services leaders are using Unit21's no-code and customizable platform to combat fraud and money laundering.

Introduction

1

For every $1 of fraud, companies lose $3.36 in chargebacks and replacement and operational costs.

With 90% of laundered money going undetected, it is difficult to gauge the actual rate of growth.

The Rising Tide of Regulation

Financial firms are dealing with unprecedented regulation and complexity. Regulatory announcements associated with fraud and AML have increased by more than 500% globally, which has led to 10-15% of total staff of financial organizations working under compliance functions. Risk management teams report spending up to 10% of revenue on compliance. As a result, globally, $213.9 billion per year is spent on maintaining financial crime compliance, which is growing at nearly 29%.[1]

This rising tide of regulation can be attributed to two increasing criminal forces: Fraud and Money laundering.

Fraud. Fraud is a costly and growing problem. For every $1 of fraud, companies lose $3.36 in chargebacks and replacement and operational costs. Identity fraud losses soared to $56 billion in 2020. Fraudsters continue to increase the scale, speed and sophistication of attacks — from 2020 to 2021, fraud grew at an average of 33% — threatening the revenue and growth of companies.[2]

Money Laundering. Meanwhile, globally money laundering is on the rise with the pandemic. With 90% of laundered money going undetected, it is difficult to gauge the actual rate of growth. The UN estimates that up to $4 trillion is laundered annually.[3] Launderers are increasingly counting on communication gaps between banks, while governments continue to try and address the threat with increasingly strict, multi-layered AML regulations.

What is more worrisome is that organized crime groups have advanced their tactics. In recent years, there has been an increase in fraud and money-laundering via:

- Creation of synthetic identities using bots and cyberattacks
- Phony e-commerce sites posing as online stores or payment providers
- The use of virtual cryptocurrencies
- Machine learning models to game traditional compliance systems
- Trade-based and cross-border laundering

[1] https://www.bloomberg.com/professional/blog/rising-compliance-costs-hurting-customers-banks-say/
[2] https://bankingjournal.aba.com/2022/01
[3] https://www.unodc.org/unodc/en/money-laundering/overview.html

A 2020 European Corporate Governance Institute report shows that stock price reactions of negative press were 9x larger than the penalties.

Financial services lose revenue due to fraud. In the case of laundering, they lose more than just money and have to answer to the government when they are not compliant.

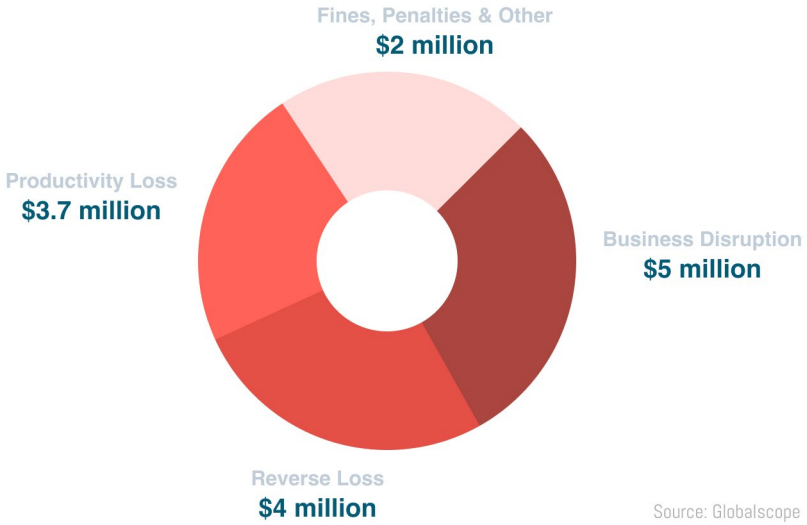
The Costs of Non-Compliance

The consequences of non-compliance are multifaceted. In 2020, AML fines exceeded USD $10 billion globally, an 80% increase over the prior year. In 2020, the SEC issued 715 enforcement actions, ordering violators to pay upwards of $4.68 billion combined. For example, in 2021, FinCEN (Financial Crimes Enforcement Network) issued Capital One with penalties of $390 million for failure to report thousands of suspect transactions.[4]

The costs of non-compliance go beyond fines.

- On average in a year, a financial organization can lose up to a total of $15 million for the consequences of non-compliance — that is 2.71x higher than what firms typically pay to stay compliant.
- A 2020 European Corporate Governance Institute report shows that stock price reactions of negative press were 9x larger than the penalties as they erode the brand, and reputation.[5]

The Costs of Non-Compliance



[4] https://www.sec.gov/news/press-release/2020-274
[5] https://www.ascentregtech.com/blog/the-not-so-hidden-costs-of-compliance/

Cryptocurrency-based crime hit an all-time high of $14 billion in 2021.

In our brand-conscious times, companies want to avoid having any association with organized crime, terrorist groups, or other criminal syndicates involved in fraud and money laundering. Compliance lapses indicate insufficient due diligence on new clients, subpar management of fraud and AML programs, poor transaction monitoring.

Why Should Fintech and Blockchain Companies Care About Financial Crime?

Fintech and Online Marketplaces

Fintechs and marketplace companies are subject to the same regulations, sanctions and fines as established financial institutions. Unfortunately, they don't have the Risk and Compliance infrastructure and headcount of large banks. Additionally, these smaller counterparts typically don't interact with their customers in-person, which complicates the ID verification process. These smaller teams must meet the compliance requirements of a sponsor bank that may not have visibility into the fintech's data. Other companies such as marketplaces and sharing-economy platforms face similar challenges, even though they don't directly engage in any financial services.

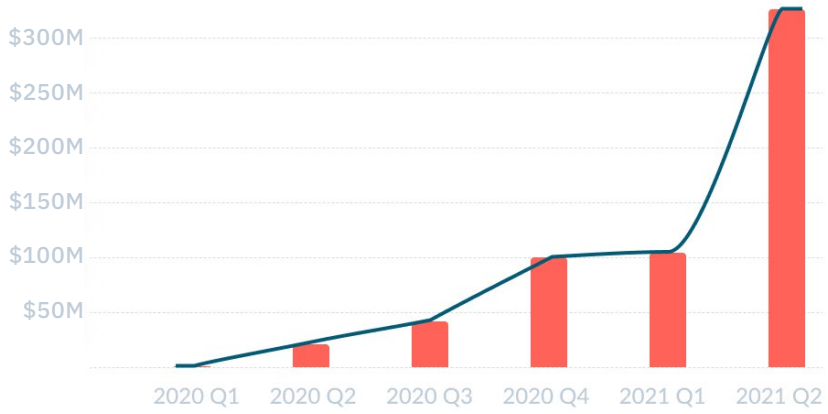
Cryptocurrency and DeFi Crime

With the increasing use of cryptocurrency, financial crime has found a new avenue. Cryptocurrency-based crime hit an all-time high of $14 billion in 2021.[6] Already, fraud is the dominant cryptocurrency crime, followed by theft. Based on blockchain technology, decentralized finance (DeFi) is the up and coming threat for fraud and money laundering. In fact DeFi hacks and fraud are on the rise as shown below.

DeFi-related hacks saw a 2.7x increase in 2021 from 2020.

[6] https://www.wsj.com/articles/cryptocurrency-based-crime-hit-a-record-14-billion-in-2021-11641500073

DeFi Hacks and Fraud are Rapidly Increasing to More Than $330M Per Quarter



DeFi hacks and fraud quarter-to-quarter, Source: Cryptocurrency Crime and Anti-Money Laundering Report, August 2021, CipherTrace

Source: CipherTrace Cryptocurrency Intelligence

FinCEN, Financial Action Task Force (FATF), and other regulatory bodies acknowledge that blockchain technology carries significant risks that we need to be wary of.

In 2020, 50% of crypto theft, totalling $118.73 million, were DeFi-related hacks. Also, in 2020, US exchanges sent $379 million of Bitcoin (BTC) directly to criminals. One third of cross-border Bitcoin volume is sent to exchanges with weak KYC (Know Your Customer).[7]

Money launderers and fraudsters existed before the advent of cryptocurrency. As the world adopts blockchain more widely, new problems will arise. The SEC, Commodity Futures Trading Commission (CFTC), and IRS have all started asserting regulatory control in the space. For example, the CFTC also has authority to regulate crypto as a commodity. The IRS has also stated that cryptocurrency investments are assets that will be treated like any other for tax purposes. Still, new capabilities and analytics may make it easier to capture bad actors and allow law enforcement professionals to examine critical cases. As crypto scams and fraud become more common, it will be important for financial organizations to help authorities with enforcement.

[7] https://fintechlegal.center/wp-content/uploads/2021/06/FLC-JFC-AMLCompliance.pdf

FRAML as an Approach — Unifying Fraud and AML Management

2

FRAML is an approach to fraud and AML that lets financial institutions address both holistically.

Looking at various financial organizations, AML and Anti-Fraud are separate. AML is often led by a Chief Compliance Officer and anti-fraud is often overseen by a Chief Risk Officer. Traditionally, they view their objectives as separate, despite the two performing similar work centered around detecting suspicious patterns, investigating system-generated alerts, and identifying criminal activity. The emergence of FRAML — i.e. Fraud + AML — reflects both the increase and interconnectedness of fraud and money laundering. FRAML is an approach to fraud and AML that lets financial institutions address both holistically. Fraud management teams and AML teams have three objectives in common:

- Finding and addressing suspicious anomalous transactions
- Shielding customers and organizations from financial crime
- Maintaining regulatory compliance

There is a major opportunity for fraud and AML teams to align behind these shared objectives. Both teams can share customer data — using a unified system to collaborate and share cases, while independently doing their own analyses.

For financial organizations, there are major benefits to using a FRAML approach:

- **Cost Savings.** Bringing these two teams into operational alignment is more cost-effective than having two disparate teams.
- **More Visibility into Financial Crime.** When the fraud management and AML teams work using the same tool, they get a broader and deeper perspective of the threats the organization faces.
- **New Capabilities for Both Fraud and AML Teams.** When fraud and AML teams share their tools, they empower one another and can collaborate on cases. Fraud teams may discover anomalous transactions that may need to be flagged for AML, and vice versa.

70% of banks are looking to achieve [fraud and AML] synergies within the next three years.

Increasing rates of financial crime are pushing teams to look at FRAML as an integrated approach with a shared end-to-end view, shared data, and a shared set of tools. Collaborating throughout the compliance and fraud value chain — from KYC and transaction monitoring to case management — financial services can increase visibility into fraud money laundering structures. Sharing information gives the ability to better understand schemes and better detect and prevent financial crimes. A study by BAE Systems reports that 70% of banks are looking to achieve synergies within the next three years, and that North American banks are typically more mature in their approach to tackling financial crime, driven by the strength of technology platforms.

Fraud and AML's Unique Obstacles

3

When you go the "build" route, engineering effectively becomes the business's bottleneck.

FRAML is easier said than done. With a variety of different tools, the outcomes can differ. More importantly, there are a few key roadblocks that are shared below:

Current Solutions and Their Shortcomings

Legacy Solutions

The transaction monitoring space for Risk and Compliance has long been dominated by legacy, on-premise providers. The software is selected by IT and Engineering departments who have control, not the compliance team. These types of implementation can take a year or more and have slow time to market. False-positive rates sometimes exceed 90%, with traditional rules systems' used by legacy compliance solutions.

The total cost of legacy platforms is also prohibitive for many smaller financial companies. Too often, AML activities are only performed periodically due to inefficiencies in processes and competing priorities. (For example, fraud solutions often get higher priority because they can prevent actual losses for a company.)

In addition, legacy solutions are limited in monitoring and analyzing large volumes of data from all daily transactions. They cannot ingest external data to provide the insights needed for a comprehensive assessment of risk. These shortcomings can lead to suspicious activities going undetected.

Homegrown Solutions

Legacy and homegrown builds may offer customization capabilities, but need more upfront work and investment. And even when implemented, they may not achieve what they are intended to do and require further interventions for customizations that come at the cost of time and resources.

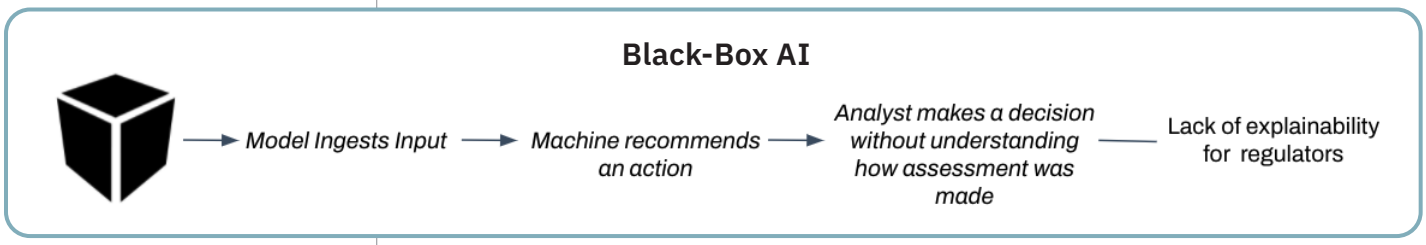
People who have built compliance tools in-house will testify that building will always take substantially longer, while the cost is exponentially higher as compliance is not their core business. The result may be a customizable but less-scalable solution for both current and future needs. What's more is, when you go the "build" route, engineering effectively becomes the

business's bottleneck. There is also a disconnect between what an operator knows vs. what engineering is building for them. This creates difficulty in optimizing workflows and resources. In such situations, customization comes at a cost and distances Risk and Compliance teams from their solution.

Newer Software Solutions

There are modern players in the fraud and AML space, many of which have more user-friendly interfaces than older incumbents. However, they are not flexible enough to codify the company's logic and rely on vendors or engineering teams for any support or updates. Fraud and AML are multifaceted but they focus mostly on transactions, providing a limited view. Additionally, they still require coding and involve teams to undertake repetitive manual tasks in processes such as Suspicious Activity Report (SAR) filing if they want to report wrongdoing. They also lack deep statistical analysis to tap into insights and do not solve for the gap between the people on the frontline who know the scenarios and rules needed, and the engineering teams who have to build them. Some tools offer black-box products with rules and models that leverage Machine Learning (ML) and Artificial Intelligence (AI). Black-box models may seem advanced and appealing, but there is little visibility into what is going on behind-the scenes — making it difficult for analysts to explain their decisions to stakeholders and regulators. While ML-based systems can be useful and drive automation, they take away control from Risk and Compliance teams to iterate on their own rules and models.

The Problem with Black-Box Models



Visibility into Fraud and AML

Too Many Datasets and Programs

There are often separate BSA (Bank Secrecy Act) and fraud departments that manage different software programs and execute their own sets of processes. This has led to operational inefficiencies where data is lost and anomalies are not properly identified. Providing critical data across multiple systems is a key first step for any fraud and AML surveillance program. This can be a beast when financial services receive low- to high-risk data from billions of transactions across different branches, and countries.

Consolidating this data is a huge barrier even the most sophisticated organizations struggle with. Fraud and BSA analysts often resort to manually compiling data to perform analysis and the siloed data makes it difficult for comprehensive analysis. Transactional data is often held in numerous legacy systems, making it difficult to connect the information, limiting the effectiveness of Risk and Compliance analysis. Financial organizations often use different vendors for KYC, transaction monitoring and case management. This means management needs to deal with multiple contracts and checks, while Risk and Compliance teams have to inconveniently toggle between different systems to detect and manage anomalous transactions.

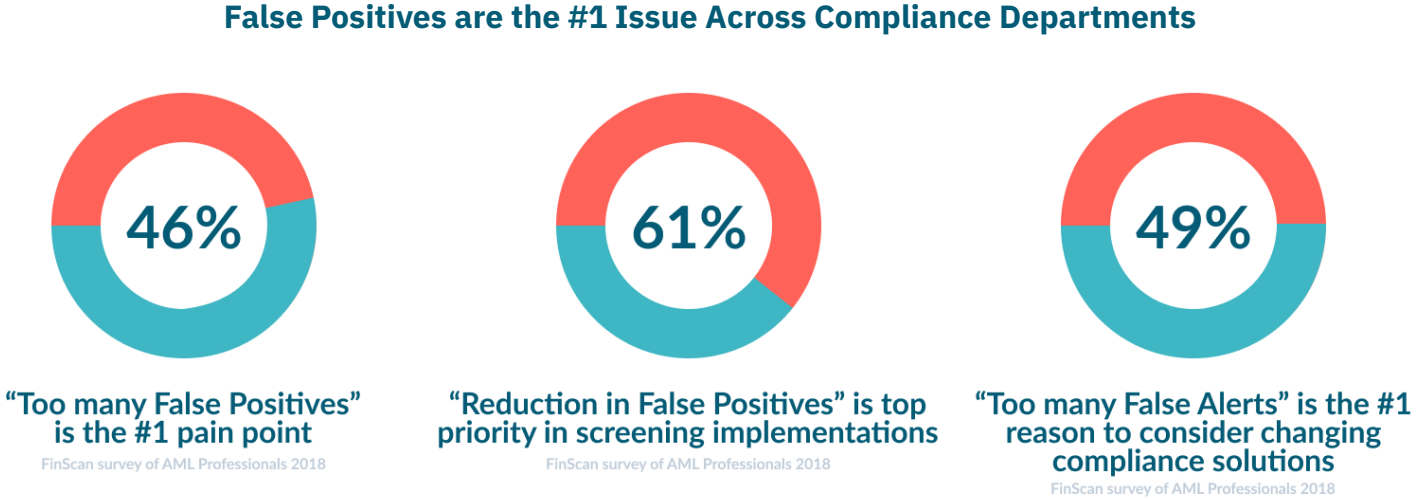
Using multiple vendors can lead to inconsistent data, disparate views and make operators prone to errors — in addition to the higher costs of installing and managing several systems. Additionally, when trying to govern and trace back data and analytics for regulators, the trails may be obscured using the different systems. Visibility is important to audit and organizations have to find ways for better data governance and transparency.

Too Many False Positives

You will not find any content on this topic that does not mention false positives. Compliance alert systems based on standard regulatory technology are triggering thousands of false positives every day. Forbes

reports that with false-positive rates sometimes exceeding 95%, something is broken with legacy compliance processes. Each of these false alarms must be reviewed by a Compliance Officer, which invites opportunities for inefficiency and human error. In traditional rule-based immutable AML models, the simpleness leads to large volumes of false positives. False positives erroneously disguise actual illegitimate activity. The direct cost alone of reviewing false positives is in the billions. Analysts investigate around 20-30 false alerts a day — decreasing productivity and capacity to focus on high-risk cases. High-volume, low-value alerts overwhelm Risk and Compliance teams.

Financial organizations have to reach out to their provider for rule-tuning, putting additional pressure on efficiency and response times. This results in higher operational costs and just higher frustration amongst analysts. In fact, AML false-positives can cost financial organizations over $3 billion every year.[8] Incumbent solutions additionally have a limited view of transaction trails whereas there are several non-monetary data streams such as user behaviors, entities and third-party data sources that may provide useful context. Such tools provide a limited foundation for anomaly detection. In addition, incumbent systems do not have the ability for testing rules and models to see what works and what doesn't. As a result, many teams work with inaccuracies, which may lead to non-compliance penalties and fraud-related losses.



False-positives are the bane of AML teams as shown in this survey of compliance professionals. Source: Dow Jones, 2018.

[8] www.forbes.com/sites/forbesinsights/2017/03/15

Risk and Compliance Operators are Far-Removed From Their Solutions

Fraud and compliance are on the front lines but often have limited influence and tools to effectively address and prevent FRAML violations.

Reliance on IT Engineering

Engineering and product teams need to hard-code software and make updates which bottlenecks processes for Risk and Compliance teams. Communication gaps and time lags between Risk and Compliance teams and Engineering may result in subpar solutions. For example, handing rules and models off to IT/engineering may lead to misinterpretations about a specification, which can lead to unnecessary back-and-forth with deployments and testing leading to communication gaps. There is often a disconnect between what an operator knows vs. what engineering is building for them. Risk and Compliance teams are better suited to create the rules and models they use for anomaly detection and investigations.

Manual, Manual, Manual

Both managers and analysts do repetitive and time-consuming administrative tasks such as alert resolution and SAR filing to regulatory authorities, and other low-value workstreams, that take away from investigating high risk transactions — or time managers could use to improve rules and models which will better flag suspicious activity. These manual processes erode operational efficiency. Case management is the key step in which fraud and AML analysts review suspicious activity. Over 2.5 million Suspicious Activity Reports (SARs) were filed to FinCEN in 2021. Although SARs are crucial to block money laundering, the system could be much more effective. Part of the challenge lies in the outdated and largely manual processes that Risk and Compliance teams use to create and submit these reports. A fraud or AML investigation can be very time-consuming and potentially futile. A compliance team is as good as its case management. The time and manual administrative work not only get expensive but can demoralize a team. If you don't have the right solution, you can task more people and still miss illegal activity. For example, US Bank used compliance software that generated too many alerts for their compliance team to handle. They continued to use the solution and capped the number of alerts that the system generated so their team could handle the workload. As a consequence, the government determined that the US bank missed a lot of suspicious activity. US Bank and its Chief Operational Risk Officer had to pay huge fines while taking a huge hit to their reputation.[9]

[9] https://www.fincen.gov/news/news-releases/fincen-penalizes-us-bank-official-corporate-anti-money-laundering-failures

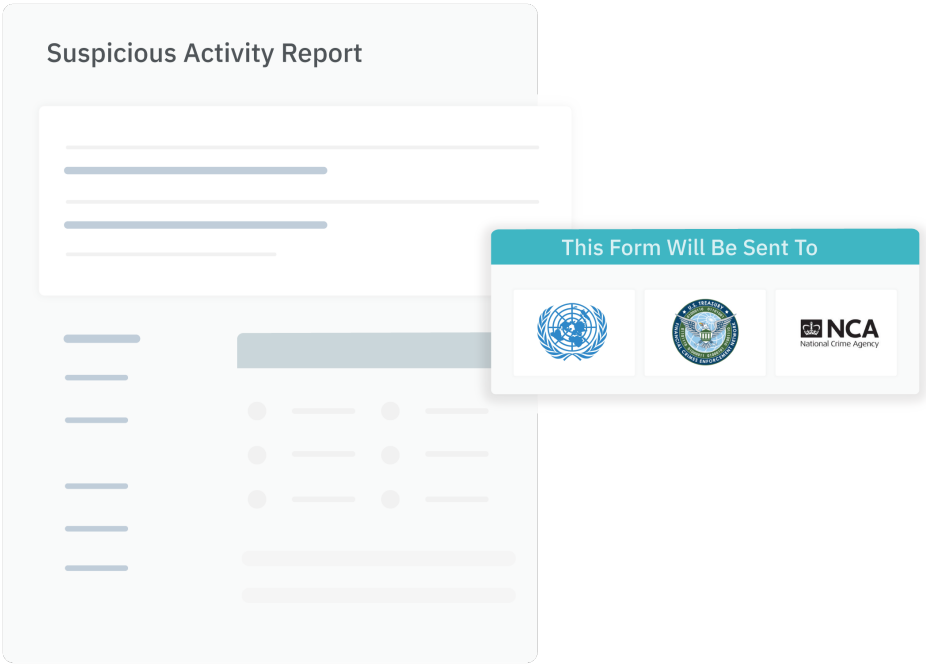
How Unit21 Approaches FRAML

4

Over 2.5 million Suspicious Activity Reports (SARs) were filed to FinCEN in 2021.

Unit21 was created to put fraud and AML operations directly in the hands of Risk and Compliance teams. It empowers teams to detect and investigate suspicious activity in a highly visible platform. Unit21 also provides pre-built rules and models to ensure you are compliant Day 1 — with the ability to customize upon those rules easily with no code. To add to Unit21's ease-of-use, it automates workflows and SAR filings so your team can focus on what matters the most. Fraud and AML teams can align behind FRAML's shared goals with Unit21. Both teams can share customer data — use a unified system to collaborate and share cases — while independently conducting analyses.

You can use Unit21's platform to manage risk compliance throughout the entire customer journey, from onboarding — to ongoing customer due diligence with identity verification, transaction monitoring, and case management. Each is key to optimizing fraud and AML operations. Let's briefly unpack each of Unit21's modular solutions.



Identity Verification or KYC/B. Identity Verification or Know your Customer (KYC) / Business (KYB) process is the first step in identifying a customer's identity and starts the risk and AML process because no further steps can be taken until the customer's identity is confirmed. The KYC process involves customer due diligence i.e. assessing the risk of doing business with the customer during both onboarding and on an ongoing basis after that.

ID Verification @Unit21. Unit21's ID Verification solution runs comprehensive KYC and KYB checks with leading data providers, Socure and Middesk, that fulfill compliance standards. The solution also automates decisions and workflows to easily onboard users and reduce friction. Additionally, get an evolving view of each customer, not just a point-in-time view, with profiles that update as user information changes and more data is collected for data monitoring.

Data Monitoring. Once the customer's identity is confirmed, the next step in fraud and AML management is transaction monitoring. This is the integral and continuous process for anomaly detection in which suspicious activity is identified and flagged.

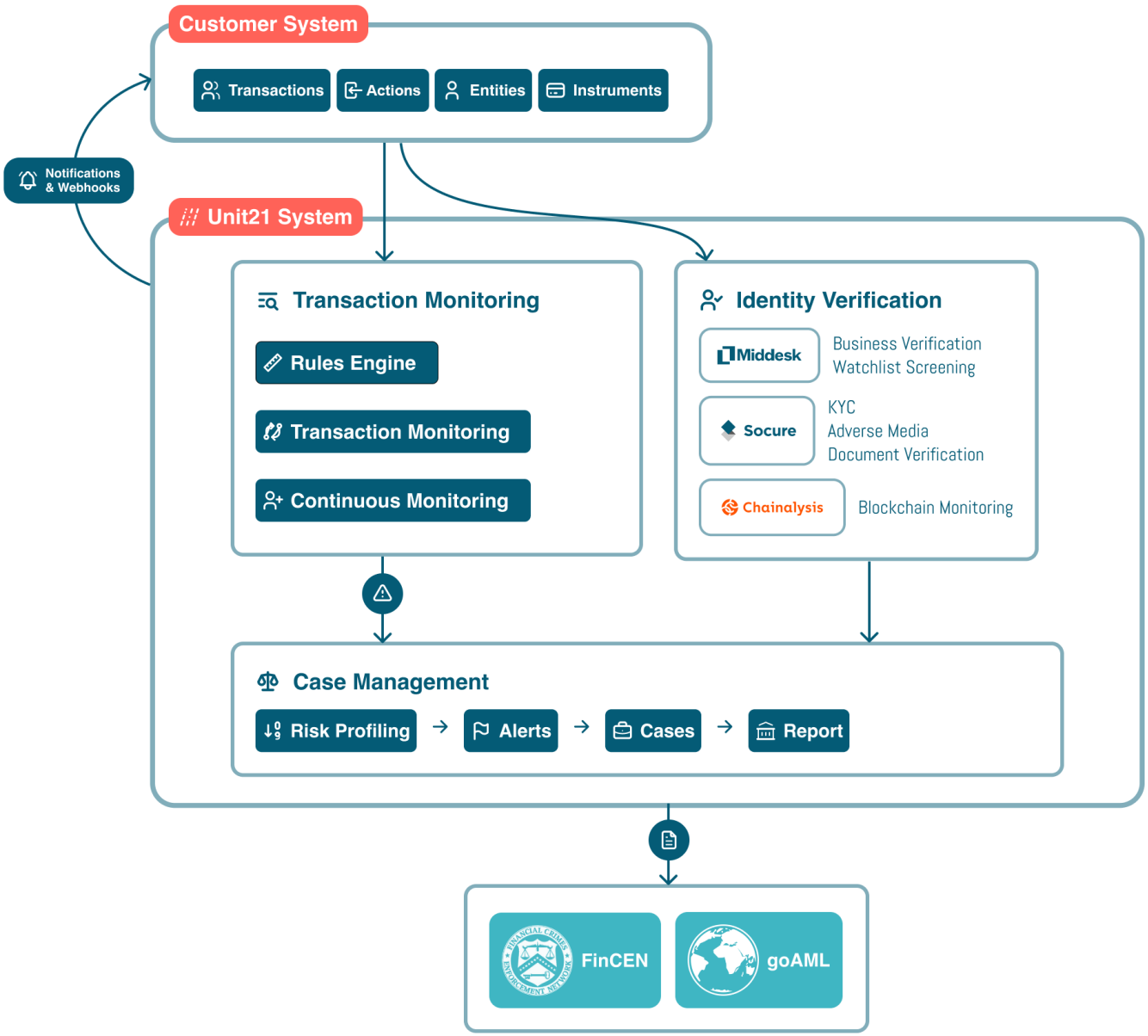
Data Monitoring @Unit21 looks at more than transactions and can monitor any data of interest in a customizable no-code environment to ensure fraud and AML teams have full control and visibility of all suspicious activity on your platform. Teams can customize rules and test rules with historical or future data to see what works to reduce false positives. The solution empowers teams to create complex and dynamic statistical models without engineering resources.

Case Management. The final part of an effective fraud and AML solution is case management. This requires analysts to review and investigate any suspicious activity that was identified by either the KYC or transaction monitoring processes.

Case Management @Unit21. Unit21 streamlines investigations with a highly customizable and automated system of record for customer risk and reviews. To make it simple, the solution also automates SAR e-filing directly to FinCEN. Connected to both Identity Verification and Transaction Monitoring, an integrated case management solution enables compliance teams to conduct their investigations far more efficiently. Unit21 also enables teams to visualize how users are connected to others using network and link analysis, and use custom risk-scores for better decision making.

Here is how Unit21 works:

First, you onboard a new user in which Unit21 lets you combine our KYC/B data sources into a single workstream and make automated decisions for identity verification. You can customize how you verify users for speed and accuracy.



Second, Unit21 customers use the rules engine to create logic or choose scenarios that will flag potentially fraudulent transactions. Options include pre-existing scenarios such as “High velocity”, “Man-in-the-middle”, “Layering”, “Abnormal volumes”, “Smurfing”, “Geography risk” and so on. Alternatively, the Unit21 rule builder allows AML agents to create highly customized logic to find fraud such as time specific “Dormancy” rules. The engine is powerful enough to recognize meme stocks, analyze NFTs, and continuously monitor actors.

Once the rules are active, Unit21 customers send their transactional data to the Unit21 system.

The data is composed of:

Entities: The parties that exchange the money on the customer platform.

Insurements: The intermediaries used by the parties to exchange the money.

Transactions: The amount of money exchanged between the parties (when/where).

Actions: Non-monetary actions a user may take such as frequent password changes.

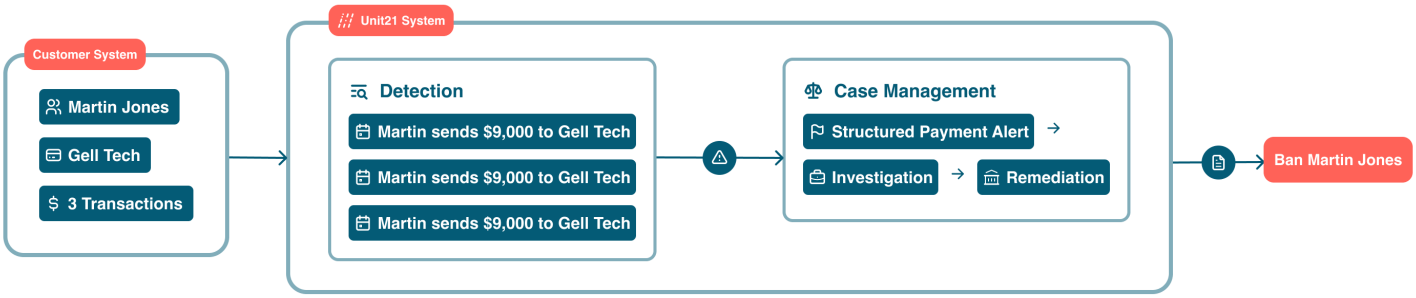
If the rules catch suspicious transactional data, AML agents will be alerted to take action.

Third, Unit21 provides a robust case management system where suspicious transactions and entities can be investigated thoroughly. Agents have the ability to whitelist entities, review historical transactions, escalate cases, create reports, and perform a link analysis. To add to Unit21’s capabilities, the platform also provides agents the ability to automatically file reports to FinCEN.

An Example

Let's take a look at a simple example. You are a Unit21 customer with a payments platform for merchants and buyers to exchange money. Today, Martin Jones is buying servers from Gell Tech using his credit card. Martin purchases the server using three structured payments. Your company sends the transaction information to Unit21 including:

Martin Jones PII	*– Name, SSN, DOB*
Martin Jones' credit card information	*– CC#*
Gell Tech PII	*– Headquarters, EIN*
Gell Tech's bank information	*– Account #*
Payment 1	*– Martin Jones $9000 -> Gell Tech @ 3:45PM on 1/21/20*
Payment 2	*– Martin Jones $9000 -> Gell Tech @ 3:47PM on 1/21/20*
Payment 3	*– Martin Jones $9000 -> Gell Tech @ 3:55PM on 1/21/20*



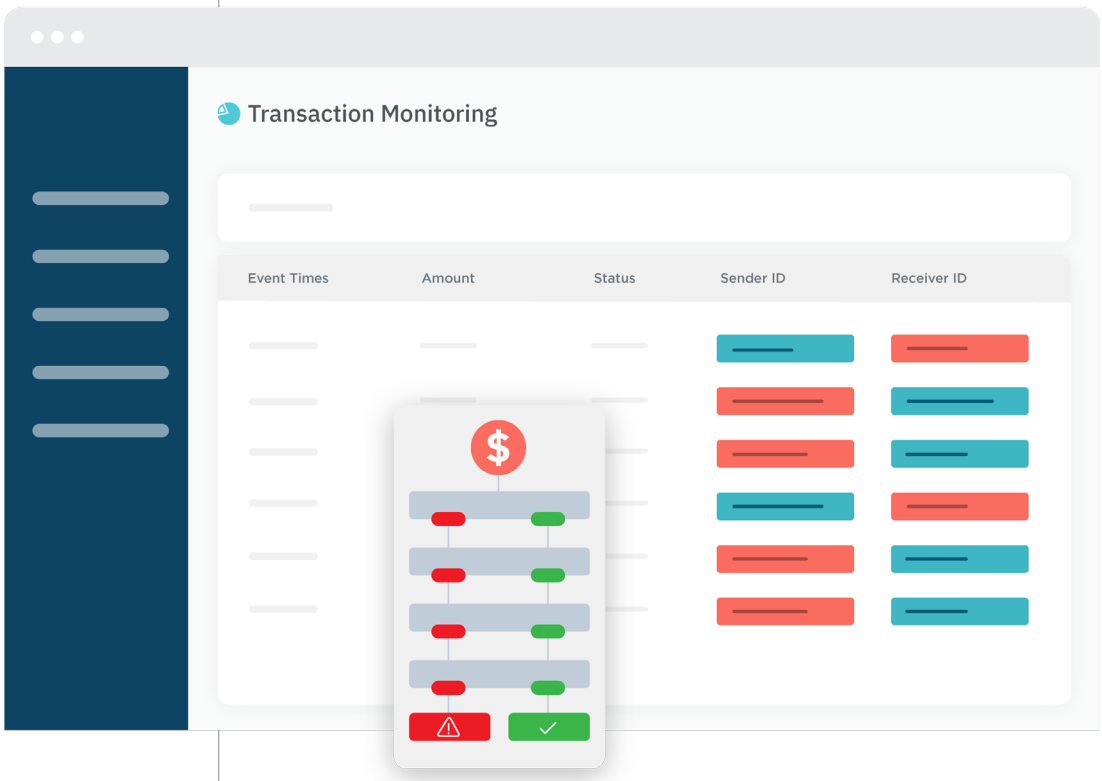
Your agents previously configured the Unit21 rules engine to flag "structured transactions". A "structured transaction" is a series of related transactions that could have been conducted as one transaction, but the financial institution and/or the transactor intentionally broke it into several transactions for the purpose of circumventing the reporting requirements of the Bank Secrecy Act (BSA).

Unit21's transaction monitoring system flags the three transactions and alerts your company. Your AML and fraud agents can use the Unit21 case management system to investigate and report Martin.

How Unit21 Empowers Fraud and AML Teams

5

Unit21 was built to empower FRAML teams. The platform helps Risk and Compliance teams in several ways.



1 Highly Visible

Look Beyond Transactions

Unit21 does more than just transaction monitoring. The solution encompasses more data and activities by bringing in actions, instruments, and entities to monitor. Test and tune rules with both historical and future data to assess what works best for more accurate anomaly detection and investigations.

An End-to-End Solution
Unit21 provides an all-in-one solution from ID verification and transaction monitoring to case management in one system. It works with consistent datasets in one consolidated end-to-end view to track users for anomaly detection and investigations. Increase visibility and provide operators with a more seamless experience to provide more accurate assessments.

Elevate Your Team
Unit21 provides management level reporting and analytics to help assess Risk and Compliance operations and team performance. Disentangle operators from the weeds so they can focus on high-risk cases.

2 Gives Fraud and AML Teams Control

Focus on Risk and Compliance, Not Engineering
Unit21 provides an easy drag-and-drop, no-code interface that can easily be used by Risk and Compliance teams — reducing reliance on engineering. Teams can tweak rules on-the-fly, and test immediately.

One-Click SAR Filing
Unit21 is intelligently automated with workflow orchestration and e-filing to regulators with integrations into FinCEN and GoAML directly from the dashboard — saving time and resources.

Accelerated Deployment with Starter Rules
Unit21 has 1,000+ tried and true, pre-built rules, models, and integrations to get started on Day 1 to meet compliance standards for your industry.

80%+

Reduction in False Positives

Quickly see a magnitude decrease in false-positive rates. Teams become more effective more they have more bandwidth to focus on what matters.

$100B+

Activity Monitored

Unit21 has monitored over $100B+ in transactions and counting. We have protected our customers against hundreds of millions of dollars of fraud loss and money laundering.

50%+

Reduction in Fraud Losses

The enhanced detection and operational efficiency afforded by Unit21 enables customers to cut fraud losses in half.

3 Agility with Customization and Automation

Purpose-Built For Your Team. By Your Team.
Easily customize rules and workflows to adapt with unique changes in company and regulations. Your compliance team who are closest to the action can define their operations. Create custom permissions and bring in your custom data with webhooks to control your Risk and Compliance approach.

Combine the Best of Customization + Automation
Unit21 provides a balance between automation and control. We provide the right rules, workflows and automation to give teams the baseline they need to get started on Day 1. Build and customize upon pre-built and automated features to continually adapt to evolving threats.

Adapt and Grow
Unit21 offers ID verification, Transaction Monitoring and Case Management on an all-in or modular basis. Unit21 enables you to seamlessly connect to its other solutions as you scale and grow — making you adaptable to your changing environment.

Customer Story:

Intuit®

"We looked at a lot of software vendors. There isn't another product that competes with Unit21. The flexibility and automation of the Unit21 platform renders completely new ways for solving problems at scale."

— Rob DeCampos, Head of BSA/AML at Intuit

Intuit has a diversified business model with a focus on innovation and providing exceptional experiences to their 50 million clients. Intuit's risk vectors have become increasingly complex as their transactions grow.

Challenges

- Transaction monitoring and case management to capture complex patterns that are more specific to Intuit's business
- Need for a high degree of automation and configurability so that teams would spend less time on manual tasks such as data aggregation and report generation, and more time on the actual investigation
- Customization would involve costly professional services hours or own internal software

Use Case

- Transaction Monitoring
- Case Management

Why Unit21?

- The ability to easily create, test, and deploy complex logic for identifying suspicious activity, without having to write any code
- The flexibility and automation of the Unit21 platform to solve large-scale problems

Impact

- 65% reduction in alert investigation times
- Used data monitoring engine to combine intelligence in anomaly detection and explainability for reporting

Customer Story:

bakkt™

"Unit21 is solving our biggest problem by monitoring hundreds of thousands of customer accounts. And the best thing is that we have been able to achieve a steady 15% false positive rate. That is a huge deal in an industry where 90-95% is the norm."

— Kailey Klein, Compliance and AML Officer at Bakkt

Bakkt is a digital asset platform that combines many different transactions with the vision to bring trust and transparency to digital assets. Bakkt unlocks the 1.20+ trillion digital assets that are currently held in crypto-currencies, rewards and loyalty points, gaming assets and merchant-stored value. Consumers can now liquidate digital assets to trade, transfer and pay in any way using Bakkt.

Challenges

- Looking for a Fraud and AML solution to accommodate the scale of their growth from 500K to 9M customers
- Spending too much time manually filing SARs; 90 minutes on each case

Use Case

- Transaction Monitoring
- Case Management

Why Unit21?

- Ease of one system and pulling reports for auditors
- Automation capabilities
- Proactive and knowledgeable customer service

Impact

- Automatic transaction monitoring with a baseline of 15% false positive rate, versus industry averages of 95%+
- Reduced SARs management time by 66% to 20 minutes

Conclusion

This ebook provides just a glimpse into some key steps that can be taken for a modern fraud and AML strategy. There is no one-size-fits-all mold, but a few key components to consider in any solution:

- The fraud and AML teams on the frontline need to be more involved in how suspicious activity is approached. While engineering is helpful to get started, they should not be a gatekeeper.
- Fraud and AML teams can benefit from sharing their data and uniting behind common objectives. Adopting an integrated FRAML approach provides for a more holistic view and cross-team collaboration and can result in significantly better detection and investigations.
- Automation and customization are integral, but there is a need to balance the two to effectively scale and respond to new threats.
- Modern tools should be data-driven, highly visible and be agile to accurately address dynamic suspicious activity.

Fraud and AML leaders are looking to bring structure and clarity to the uncertainty surrounding them. Empowering teams under a highly effective FRAML system with modern Risk and Compliance tools can bring the confidence to better understand and preempt bad actors.

What's Next?

To check out a demo or learn more about how Unit21 can help you, **schedule a consultation**. You can stay up to date on the latest events, case studies, and solutions for financial services at **https://www.unit21.ai**

Unit21 is the only customizable no-code platform for Risk and Compliance operations, empowering companies with automation, control and visibility in their battle against fraud and money laundering. Backed by Google, Unit21 helps over 100 fintechs and crypto platforms create and iterate their own rules and models, without having to send them off to engineers. **Schedule a demo today** to see our platform in action.

343 Sansome Street, Suite 1600
San Francisco, CA 94104