

A Guide to Risk-Aligned Transaction Monitoring

How to cut false positives and move from alerts to decisions faster

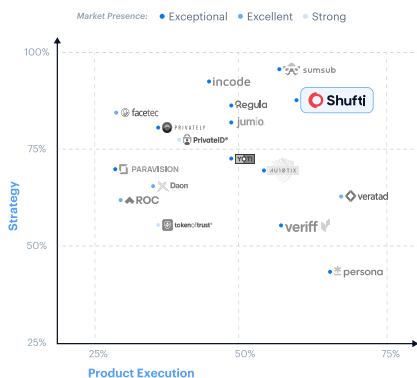


Industry Recognition 2025–2026

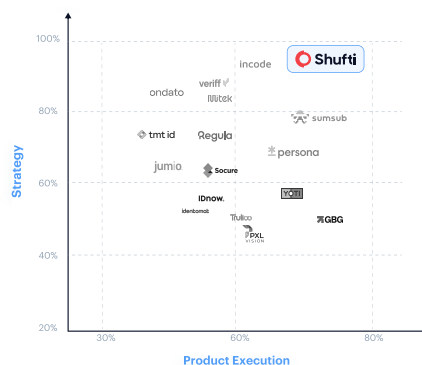
Recognised by leading analyst firms, government bodies and independent research organisations



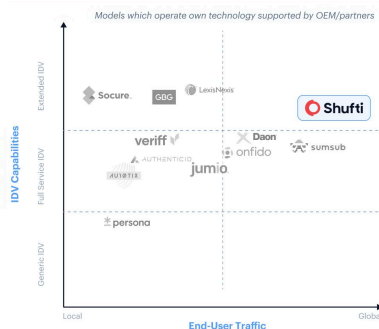
Ranked Exceptional in Liminal's 2026 Age Estimation Index



Ranked Exceptional in Liminal's 2026 Age Verification Index



Broadest global reach in the 2025 KuppingerCole Extended IDV report



Recognised as a Leader across four G2 Summer 2026 reports



Differentiated by Gartner on document diversity and country coverage



240+
Countries
& Territories

10k+
Document
Types



First EU company to achieve iBeta Level 3 Conformance to ISO/IEC 30107-3, with 0% APCER

**iBeta Level 3
Conformance**
0% APCER



Ranked Top 5 in the DHS RIVR 2025 for identity validation

0%
Extraction
Failure

0.67%
Worst-Case
FNMR





What this guide covers

Contents

·	Introduction	03
01	Transaction monitoring, fraud detection and where they overlap	04
02	How transaction monitoring works	08
03	Transaction monitoring challenges across financial services models	10
04	What regulators require from transaction monitoring	13
05	Beyond transactions threshold- detecting financial crime risk	20
06	Where compliance officers face challenges with transaction monitoring solutions	28
07	How financial regulators expect transaction monitoring solutions to operate	32
08	How to choose the right transaction monitoring solution	37
09	AI-powered monitoring for risk scenario alignment and compliance	44
·	References	51

Introduction

A recurring challenge in AML compliance for financial service providers is effective transaction monitoring. As transaction volumes grow, payment rails become faster and financial-crime typologies evolve, monitoring programmes can struggle to keep detection aligned with the institution's actual risk exposure. Static thresholds, limited contextual data and slow scenario adaptation can leave suspicious activity undetected, while poorly designed or calibrated scenarios can generate false-positive alerts that increase investigation workload and compliance costs.

The challenge becomes more complex for organisations such as payment service providers and marketplaces that facilitate payments, where transaction monitoring may operate alongside fraud detection. The same activity can carry both fraud and money-laundering indicators, making it important to assess transaction behaviour alongside customer context, counterparties and other relevant risk indicators rather than relying on individual signals in isolation.

FINMA's on-site supervisory reviews conducted in 2024 found similar weaknesses. At some supervised institutions, transaction monitoring systems lacked an appropriate combination of static and dynamic criteria or scenarios, which contributed both to suspicious transactions being missed and to large numbers of false-positive alerts. FINMA also identified room for improvement in the criteria used for higher-risk transactions and business relationships, and expects institutions to align those criteria with their specific risks. ^[1]

The consequences of these gaps can be significant. In the 2024 TD Bank enforcement case, the US Department of Justice found that the bank added no new transaction-monitoring scenarios and made no material changes to existing scenarios from at least 2014 through late 2022, despite emerging risks and new products and services. From 1 January 2018 to 12 April 2024, 92% of its total transaction volume was outside its automated transaction-monitoring system, representing approximately \$18.3 trillion in activity. ^[2]

For financial service providers, the challenge is therefore not simply to monitor more transactions, but to monitor the relevant risks with sufficient context. Weak scenario alignment can leave exposure undetected, while excessive false positives consume analyst capacity and increase the operational burden of compliance.

An effective transaction monitoring solution should therefore support risk-aligned scenario configuration, contextual detection, timely investigation and more precise, auditable and defensible compliance decisions.

Transaction Monitoring, Fraud Detection and Where They Overlap

What is the Transaction Monitoring

Transaction monitoring is the ongoing review of customer transactions after onboarding, to identify activity that may indicate money laundering, terrorist financing or sanctions exposure. It is a continuing obligation across the life of the customer relationship rather than a check performed once, and it covers deposits, withdrawals, transfers, payouts and refunds. Effective transaction monitoring also extends to non-payment data such as logins, password recovery attempts and account detail changes, along with changes in device and IP, because those carry the signals that identify account takeover and money mule recruitment.

A transaction can be monitored for its risk exposure not only against a value or a rule, but against what the institution already knows about the customer: their profile, financial activity, their risk rating and their established Transaction Behavior.

— FIGURE 01

What transaction monitoring reviews

PAYMENT DATA



Deposits



Withdrawals



Transfers



Payouts



Refunds

NON-PAYMENT DATA



Logins



Password recovery attempts



Account detail changes



Changes in device and IP

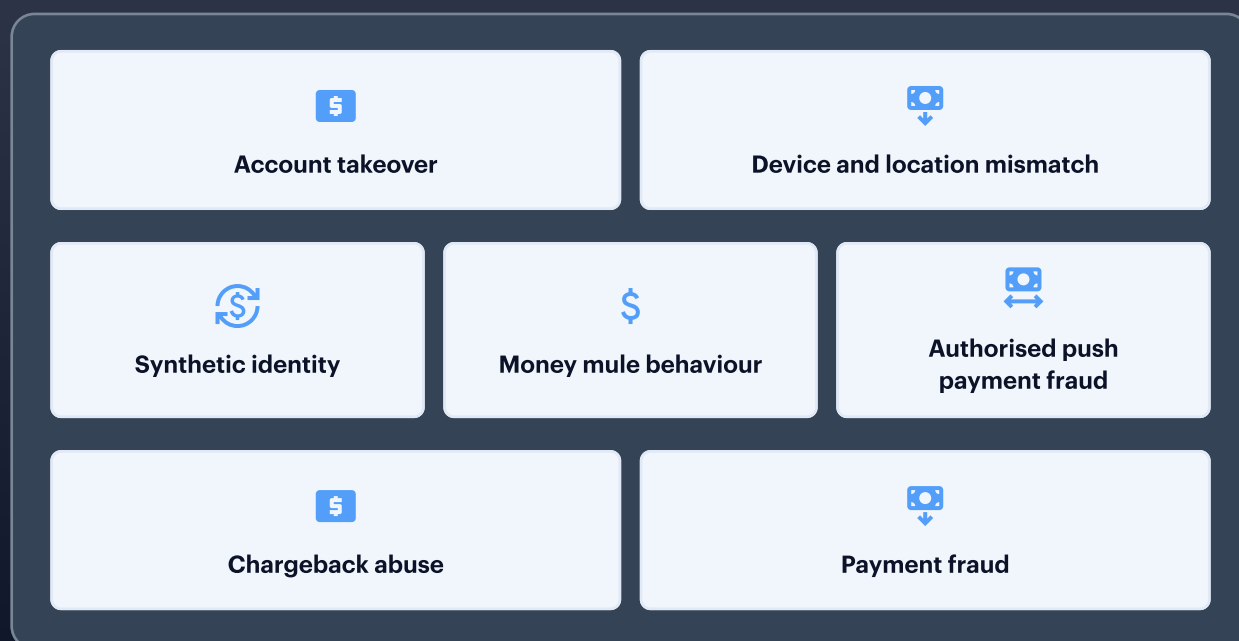
BOTH CARRY THE SIGNALS THAT IDENTIFY ACCOUNT TAKEOVER AND MONEY MULE RECRUITMENT

What is fraud detection?

Fraud detection assesses whether the person conducting a transaction is who they claim to be, and whether they intend it. It covers account takeover, device and location mismatch, synthetic identity, money mule behaviour, authorised push payment fraud, chargeback abuse and payment fraud.

— FIGURE 02

What fraud detection covers



The distinction is one of question rather than technique. AML Transaction monitoring asks whether money is criminal in origin or destination. Fraud detection asks whether the transaction itself is legitimate and authorised. Assessment of both of these risks, requires diverse data sets which includes a customer's identity data, Sanctions and PEP Risk, Source of Income, and other indicators related to purpose of account, expected transaction volume expected from the kind of profile.

Same transaction, two questions

— FIGURE 03

AML transaction monitoring and fraud detection compared

	AML TRANSACTION MONITORING	FRAUD DETECTION
Core question	Is this consistent with what we know about the customer, and does it match a laundering typology?	Is this person who they claim to be, and do they intend this transaction?
Typical signals	Structuring, corridor risk, beneficiary changes, sanctions exposure, transaction velocity	Device mismatch, IP anomaly, account takeover, synthetic identity, mule behaviour
Primary obligation	Report suspicion to the Financial Intelligence Unit	Prevent loss and protect the customer
Typical timing	Real time and post-transaction review	Usually real time, at or before authorisation
Usual owner	Compliance function and MLRO	Fraud or risk team

WHERE THE TWO MEET

Money-mule activity and authorised push payment fraud generate signals relevant to both disciplines. Certain typologies are difficult to assess when fraud and AML signals are viewed in isolation.

Where do transaction monitoring and fraud detection overlap?

Fraud and money laundering are distinct financial-crime risks, but certain crime typologies can produce signals relevant to both. Money-mule activity is one such example, where fraud detection and transaction monitoring may need to work together to identify how criminal proceeds are received, moved and dispersed through customer accounts.

A notable supervisory example is the FCA's work on money-mule detection, which has highlighted the importance of controls spanning onboarding, fraud indicators, transaction monitoring and suspicious activity reporting. [\[3\]](#) [\[4\]](#) This does not mean every fraud event becomes an AML case, but it does show why some typologies are difficult to assess when fraud and AML signals are viewed in isolation.

Authorised push payment fraud presents a similar progression. The payment may initially appear as a fraud event for the sending institution, while the receiving account and subsequent movement of funds can generate indicators associated with mule activity and laundering of criminal proceeds.

Monitoring may operate pre-transaction, in real time, near-real-time or post-transaction depending on the control objective, applicable framework and sector-specific requirements. Some suspicious patterns become identifiable only when later transactions, customer behaviour or linked-account activity provide additional context.

How Transaction Monitoring Works

A transaction monitoring programme runs as a connected sequence, where every stage depends on what the stage before it supplied.

— FIGURE 04

How Transaction Monitoring Works end to end



Transaction Monitoring End to End

What each stage supplies to the next

Onboarding and data ingestion

The sequence starts at onboarding. The verified identity, KYC outcome, screening status and customer risk rating established there become the baseline every later stage assesses against, and without them monitoring assesses an account number rather than a known customer. Transaction records then arrive from the institution's payment rails, where they are enriched with customer, beneficiary, device and merchant attributes and normalised so detection logic can reference them reliably.

Detection in real time and after settlement

Detection itself runs at two points in time. Transactions are scored against deployed scenarios as they occur, which allows the institution to decline, hold or approve before settlement where the control objective requires it. Cleared activity is then reviewed again once later transactions supply context, catching sequences that no single transaction would reveal.

Alert prioritisation, investigation and decision

What follows determines what a human sees. Alerts are scored, ranked by risk relevance and routed to the appropriate review tier, and a programme that skips prioritisation sends everything to one queue in arrival order. Context is then assembled, evidence is recorded, and the case moves through analyst tiers under review controls and service level tracking, until the accountable decision-maker determines whether the activity is reportable and records that determination with its supporting rationale.

Reporting and the feedback loop

Once that determination is made, the case should move into the jurisdiction-specific reporting workflow. This can include generating the required SAR or STR fields, attaching the relevant transaction and customer context, and submitting through the prescribed FIU channel or schema, for example goAML for certain jurisdictions. What the investigation established then updates the customer risk rating and the expected activity profile, which changes what monitoring looks for next. Where this loop is absent, the programme keeps assessing customers against a profile it has already disproved.

Transaction Monitoring Challenges Across Businesses Sectors

There is no single transaction monitoring configuration that fits the need for every business or matches their risk exposure.

The data available, transaction structure, customer relationship and financial crime typologies change with the business model. A monitoring platform therefore has to adapt not only its thresholds, but also the scenarios, data points and relationships it evaluates.



Banks and financial institutions

For banks, transaction monitoring has to account for the breadth of activity as per the exposure created by the institution's product mix and payment infrastructure. Each product can generate different transaction patterns, counterparties, velocity profiles and geographic risks, requiring monitoring scenarios and thresholds to adapt to the underlying product and payment type.

WHERE EXPOSURE DIFFERS

- Current and savings accounts
- Consumer and commercial lending
- Trade and asset finance
- Correspondent banking
- Card, wire and ACH payments



Fintechs and neobanks

For fintechs and neobanks, transaction monitoring has to adapt to rapid customer acquisition, remote onboarding and increasingly diverse product sets. Exposure can include newly opened mule accounts, rapid movement of incoming funds, fiat-to-crypto conversion, multiple-device activity and sudden changes in behaviour before a mature transaction history has formed.

WHAT THE PLATFORM MUST COMBINE

- Identity and CDD information
- Customer risk
- Device and geolocation
- Fiat and crypto activity
- Velocity and behavioural change



Payment service providers

A payment service provider may need to understand more than the payer and the individual payment. Instant payment rails also require monitoring to operate in real time, as suspicious activity may need to be assessed before the payment is settled or becomes irrevocable.

NEEDS VISIBILITY INTO

- Merchant identity
- Expected transaction profiles
- Counterparties
- Geography
- The payment flow itself



Marketplaces and platform businesses

For marketplaces that process or facilitate payments, risk often emerges from the relationship between the buyer, seller, payment method, device and transaction history rather than from the value of an individual payment. Seller identity, payment behaviour, device signals and relationship data become particularly important where individual transactions appear legitimate in isolation.

PATTERNS TO IDENTIFY

- Unusually high dispute rates
- Refund-and-repurchase activity
- Abnormal chargeback volumes
- Coordinated activity across accounts
- Account Take-Over



Crypto businesses and virtual asset service providers

For virtual asset service providers, the relevant transaction does not end at the customer account. Risk can sit in the wallet, blockchain history, counterparty VASP or an unhosted wallet outside the institution.

WHERE THE RISK SITS

- The wallet
- Blockchain history
- Counterparty VASP
- Unhosted wallets
- Travel Rule information



Remittance operators and exchange houses

For remittance operators and exchange houses, transaction monitoring has to recognise risk patterns that are specific to high-volume, cross-border and often cash-funded transfers. This becomes especially visible in regulatory guidance from jurisdictions with large migrant-worker populations, including Gulf markets.

WHAT MONITORING MUST SEE

- Value inconsistent with customer standing
- Activity outside normal business
- Unnecessarily complex transactions
- Ordering and beneficiary sides



iGaming operators

For gambling operators, transaction value alone is an inadequate monitoring threshold. Monitoring therefore needs to follow activity across payment methods and over time, increasing the depth of scrutiny as customer risk changes.

SIGNALS THAT ALTER RISK

- Deposits and withdrawals
- Multiple payment methods
- Source of funds
- Open-loop payments

What Regulators Require From Transaction Monitoring

Monitoring obligations come from three levels: the standards set by Financial Action Task Force, the regional framework, and the national regime that implements it. They do not impose identical requirements, and a multi-jurisdictional institution has to satisfy each on its own terms.

— FIGURE 05

Three levels of requirement

FATF standards

The international baseline most national regimes implement



Regional frameworks

Directives and regulations applying across a bloc



National regulations

United Kingdom · United States

FATF Recommendations

The FATF Recommendations set the international baseline for transaction monitoring that most national regimes implement. Five requirements bear directly on transaction monitoring.

- **Ongoing due diligence throughout the relationship.** Scrutiny of transactions undertaken throughout the course of the relationship to ensure they remain consistent with the institution's knowledge of the customer, their business and risk profile, and, where necessary, their source of funds.
- **A risk-based approach.** Institutions identify, assess and understand their money laundering and terrorist financing risks and apply measures proportionate to those risks.
- **Keeping transaction and customer records.** Necessary records on domestic and international transactions, together with information obtained through customer due diligence, are retained to support ongoing monitoring, investigation and regulatory requirements.
- **Payment transparency.** Required originator and beneficiary information accompanies relevant transfers, providing the information needed to identify and trace parties involved in payment activity.
- **Reporting suspicion promptly.** Where an institution suspects, or has reasonable grounds to suspect, that funds are the proceeds of criminal activity or are related to terrorist financing, it reports its suspicions promptly to the Financial Intelligence Unit.

Predicate Offences- FATF

FATF Recommendation 3 requires countries to criminalise money laundering on the basis of the Vienna and Palermo Conventions, and to apply the offence to all serious crimes with a view to including the widest range of predicate offences. The designated categories of offences span trafficking in persons and migrant smuggling, illicit trafficking in narcotic drugs, fraud, counterfeiting, corruption and bribery, tax crimes, insider dealing and market manipulation, and environmental crime.

Where predicate-offence risks are material to an institution's business, customers or geographic exposure, obligated sectors may need to tune Transaction monitoring rules to the underlying threat typologies rather than rely on generic transaction thresholds. This can mean translating known laundering methods into relevant indicators, scenarios and escalation logic so monitoring remains aligned with the risks identified.

European Union

Current framework. Ongoing monitoring obligations currently derive from Directive (EU) 2015/849, as amended, and its national transpositions. Obligated entities must scrutinise transactions throughout the business relationship to ensure that activity remains consistent with what they know about the customer, the customer's business and risk profile, while keeping relevant customer information up to date. National implementation still determines matters such as supervisory practice, reporting channels and certain procedural requirements.

Predicate offences. Directive (EU) 2018/1673 establishes minimum criminal-law rules for money laundering and defines the criminal activity capable of constituting predicate offences through penalty thresholds and a set of designated offence categories. Member States may retain or adopt broader criminal-law definitions. Criminal offences affecting the Union's financial interests are governed separately by Directive (EU) 2017/1371.

— FIGURE 06

The EU monitoring obligation, before and after 10 July 2027

CURRENT Directive (EU) 2015/849, as amended

Ongoing monitoring obligations derive from the Directive and its national transpositions. National implementation determines supervisory practice, reporting channels and certain procedural requirements.

FROM 10 JULY 2027 Regulation (EU) 2024/1624 applies directly

Article 26 requires ongoing monitoring of business relationships and customer transactions. Article 77 establishes a directly applicable five-year retention period.

Direct application, reporting and retention

From 10 July 2027. Regulation (EU) 2024/1624 applies directly across Member States. Article 26 requires ongoing monitoring of business relationships and customer transactions so that activity remains consistent with the obliged entity's knowledge of the customer, business activity and risk profile, and requires relevant customer information to be kept up to date. Recital 72 further describes effective monitoring as risk-based and designed around precise and relevant criteria reflecting customer characteristics, risk level, products and services, and relevant countries or geographical areas.

SAR Reporting. Obligated entities must promptly report relevant suspicions to their national Financial Intelligence Unit. The current EU framework requires CDD documents and transaction records to be retained for five years, subject to limited extensions under national law.

Record Maintenance. From 10 July 2027, Article 77 of Regulation (EU) 2024/1624 establishes a directly applicable five-year retention period, with competent authorities able to require further retention of up to five years where justified.

United Kingdom

Framework. The Money Laundering Regulations 2017 require ongoing monitoring of business relationships, including scrutiny of transactions to ensure that activity remains consistent with the firm's knowledge of the customer, their business and risk profile. The Proceeds of Crime Act 2002 provides the principal criminal-law and suspicious activity reporting framework, as subsequently amended by measures including the Economic Crime and Corporate Transparency Act 2023.

SAR Reporting. Where the statutory conditions under POCA are met, relevant suspicions must be disclosed to the National Crime Agency. ECCTA 2023 introduced targeted changes to the wider reporting framework, including strengthened information-gathering and information-sharing provisions, while the underlying obligation to report relevant suspicions remains in place.

Records. Customer due diligence information and supporting transaction records are generally retained for five years under the Money Laundering Regulations, subject to the detailed statutory retention rules.

— FIGURE 07

The UK framework in three instruments

MONITORING

MLR 2017

Ongoing monitoring of business relationships

CRIMINAL LAW

POCA 2002

Principal criminal-law and SAR framework

AMENDING

ECCTA 2023

Information-gathering and sharing provisions

United States

Framework. FinCEN administers regulations under the Bank Secrecy Act, which requires covered institutions to maintain an effective AML programme with policies, procedures and internal controls covering customer identification, reporting, recordkeeping and response to law enforcement requests.

SAR Reporting. A suspicious activity report is generally due within 30 calendar days of initial detection of facts that may constitute a basis for filing, extending to 60 days where no suspect can initially be identified.

Records. BSA records are retained for five years and must be available to FinCEN and other law enforcement or supervisory agencies on request.

— FIGURE 08

Reporting deadlines are not equivalent

UNITED STATES	UNITED KINGDOM	EUROPEAN UNION
30 days	As soon as practicable	Promptly
From initial detection, extending to 60 days where no suspect can initially be identified	Once the statutory reporting conditions are met	To the national Financial Intelligence Unit

A MULTI-JURISDICTIONAL INSTITUTION HAS TO SATISFY EACH ON ITS OWN TERMS

Beyond Transactions Threshold- Detecting Financial Crime Risk

An institution's financial crime risk assessment identifies which crimes its customer base, products and markets expose it to.

Converting that identification into working detection means turning a description of criminal conduct into logic a transaction monitoring platform can execute against transaction data, and that conversion is where most detection coverage is lost.

Why Detection of Only Transaction Thresholds Is No Longer Sufficient

Traditional transaction monitoring was built around transaction thresholds and a narrow set of generic money laundering typologie, like structuring, smurfing, round-amount transfers, velocity breaches, activity just below a reporting limit. Those scenarios detect the mechanics of laundering. They describe how money is moved to avoid attention, not which crime produced it.

Evolving Crime Typologies

The range of crimes a monitoring programme is expected to detect has widened. FATF's designated categories of offences now span trafficking in persons and migrant smuggling, environmental crime, tax crimes and market manipulation alongside the drug trafficking and corruption offences the earliest frameworks were written around, and each of those crimes produces a different pattern once the proceeds enter the financial system.

Financial Products with Higher Risk Exposure

The products carrying that risk have changed as well. Instant payment rails, e-money and prepaid instruments, virtual assets, embedded finance and marketplace payouts move funds faster, across more parties, and with less customer history behind each transaction than the account-based products the generic scenarios were calibrated on. A structuring threshold written for branch cash deposits says little about a marketplace seller network or a chain of transfers settled in ten seconds.

Supervisory expectation has moved with both. Suspicious activity reports are increasingly expected to connect the activity observed to the predicate offence it may relate to, and Financial Intelligence Units now publish offence-specific indicator sets to support exactly that connection.

The obligation is to identify unusual or suspicious transactions and patterns in line with the ML/TF risks to which the institution is exposed, taking into account the customer's risk profile and the institution's knowledge of the customer.

Detecting financial activity consistent with proceeds of crimes such as terrorist financing, human trafficking, migrant smuggling or investment fraud depends on combinations of transaction, customer, counterparty, merchant, device, location and historical attributes assessed together, not on merely tuning a financial threshold limit up and down. Where a monitoring solution cannot ingest and evaluate those data points, the right risk scenario can't be analyzed, and the institution files reports describing unusual transactions rather than suspected offences.

38%

of reported terrorist-financing control weaknesses involved either **missing transaction-monitoring scenarios** or monitoring systems that failed to detect TF.

EUROPEAN BANKING AUTHORITY, JULY 2025

The European Banking Authority (EBA) identified clear gaps in scenario-aligned transaction monitoring in its 2025 Report on Money Laundering and Terrorist Financing Risks Affecting the EU's Financial Sector, published on 28 July 2025. Drawing on supervisory information from competent authorities responsible for overseeing financial institutions across the EU, the EBA found that 38% of reported terrorist-financing control weaknesses involved either missing transaction-monitoring scenarios or monitoring systems that failed to detect TF. In some cases, institutions exposed to significant TF risk had not configured scenarios to consider indicators such as low-value transactions, showing how monitoring gaps can emerge when rules and thresholds are not aligned with the specific risk scenario.

Monitoring Transactions to Detect Suspicious Activities

The clearest illustration of that expectation comes from the FIUs themselves. Canada's FINTRAC has published offence-specific indicator sets that show precisely what it expects reporting entities to be able to see, and the example below concerns one predicate offence in particular, including human trafficking for sexual exploitation.

Takeaway from Canadian Financial Intelligence Unit

FINTRAC Operational Alert FINTRAC-2021-OA001, published in July 2021 in support of Project Protect, sets out updated money laundering indicators associated with human trafficking for sexual exploitation. FINTRAC based the alert on an analysis of approximately 100,000 transactions disclosed between 2018 and 2020.

The indicators demonstrate the level of detail that transaction monitoring may need to evaluate. FINTRAC identified patterns involving email money transfers, cash deposits, prepaid credit cards, gift cards, online casinos, virtual currencies, related accounts, nominees and front companies. ^[5]

100,000

transactions disclosed
between 2018 and 2020,
analysed for the alert

2018–2020

the period over which those
disclosures were made

2021

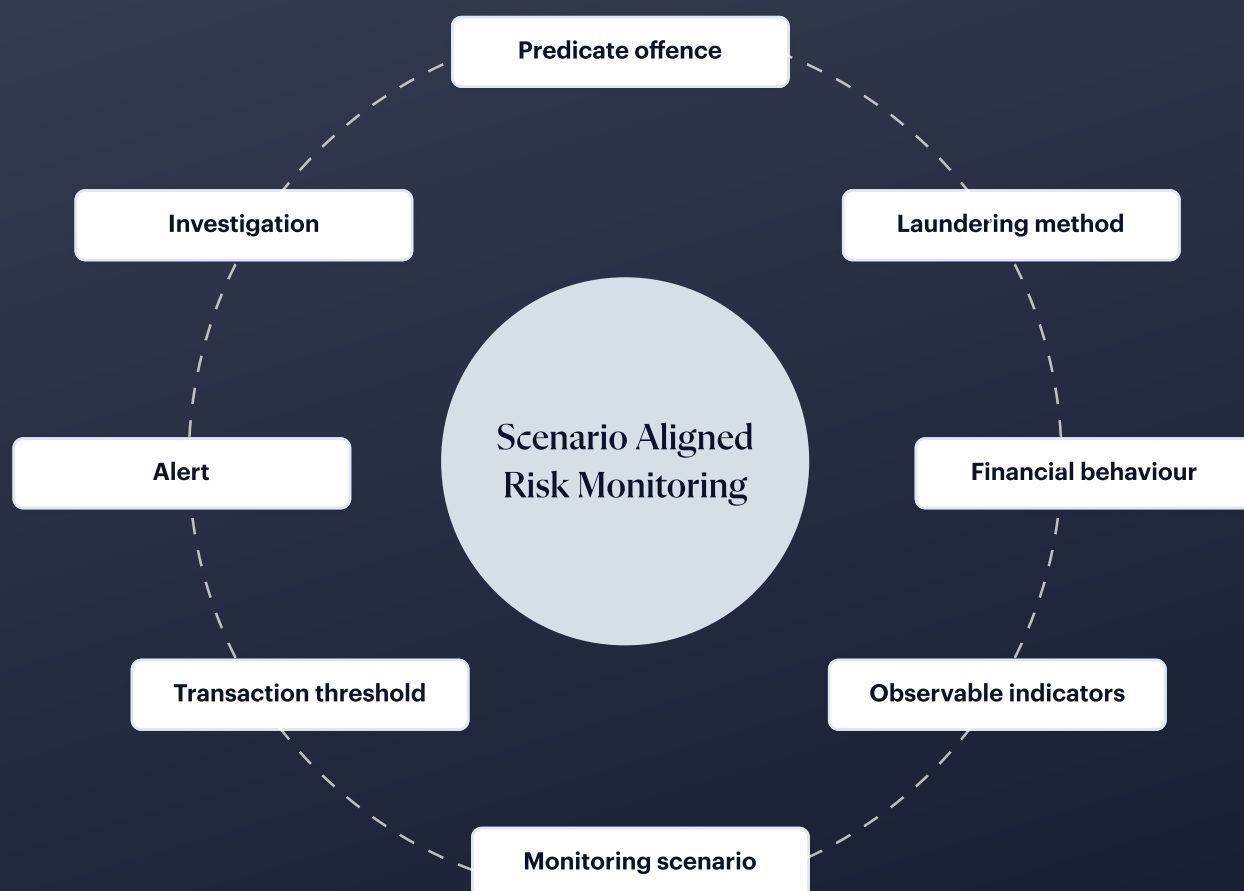
Operational Alert FINTRAC-
2021-OA001, published in
support of Project Protect

The financial crime risk to suspicious transaction scenario translation

The translation runs in one direction, from the offence an institution is exposed to through to the investigation that follows an alert. Each transition discards information: a laundering method describes less than the offence, an indicator less than the behaviour, and a threshold less than the indicator. By the time the sequence reaches an alert, the detection logic is operating only on what survived every earlier step.

— FIGURE 09

Risk-to-scenario framework



Some of the Common Financial Crime Scenarios in Transaction Monitoring

Here are some of the common financial crime scenarios that a financial service provider may need to detect.

FIVE SCENARIOS AND WHAT EACH LOOKS LIKE IN THE DATA



Migrant smuggling produces payments staged along a route rather than settled in one movement, remittances routed through intermediary jurisdictions, and cash collection at transit points involving individuals with little other financial history. [\[6\]](#) [\[7\]](#) [\[8\]](#)



Drug and fentanyl trafficking produces structured cash deposits below reporting levels, funnel account activity where deposits made in several locations are withdrawn in another, trade-based laundering through mis-invoiced goods, and payments for precursor chemicals that present as ordinary commercial transactions. [\[9\]](#) [\[10\]](#)



Cyber-enabled and investment fraud presents the hardest detection case, because the customer conducting the transaction is the victim. The payments are authorised, legitimately funded and instructed by the account holder. What identifies them is escalation in value over weeks, transfers to recently opened accounts or crypto-asset service providers, liquidation of savings, and departure from the customer's own established transaction behaviour. [\[11\]](#)



Sanctions evasion produces routing through intermediary jurisdictions without commercial rationale, layered ownership structures obscuring the ultimate counterparty, re-invoicing, and payment flows deliberately separated from goods flows. [\[12\]](#) [\[13\]](#)



Export-control evasion. For financial institutions exposed to international trade, transaction monitoring may also need to identify activity linked to export-control evasion, particularly where customers trade defence, advanced-technology or dual-use goods. FinCEN and the U.S. Bureau of Industry and Security have issued specific red flags for transactions involving dual-use products, including payments routed through newly formed intermediary companies, sudden increases in purchases of controlled goods, smaller payments from one end user to multiple suppliers, and customers unwilling to disclose the end user, intended end use or ownership structure. [\[14\]](#) [\[15\]](#) [\[16\]](#)

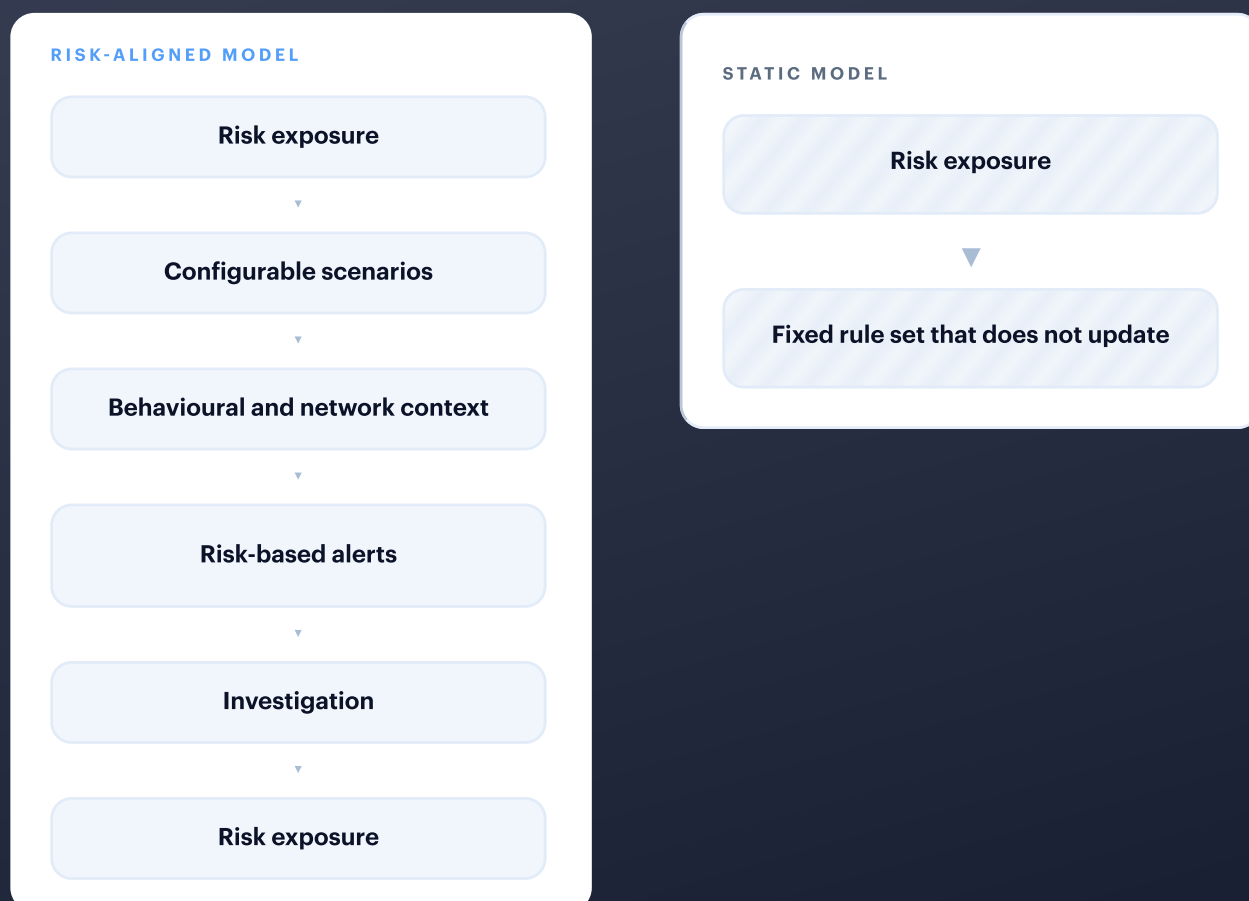
Challenges Businesses Face in Scenario-Aligned Transaction Monitoring

The effectiveness of transaction monitoring depends not only on the rules a platform can base its risks on, but on the breadth of data those rules can evaluate to detect actual risks. Detecting suspicious activity associated with predicate-offence typologies often requires analyses of the multiple data points, which include the combinations of transaction, customer, counterparty, behavioural, merchant, device, location and historical attributes.

Where a monitoring solution can access only a limited set of data points, it may be unable to reproduce that level of detection logic, leaving genuine suspicious patterns undetected while generating alerts on activity that lacks the wider context needed for accurate assessment.

— FIGURE 10

Modern detection model



SAME STARTING POINT, DIFFERENT AMOUNT OF CONTEXT REACHING THE ANALYST

Typologies that never become deployed scenarios

Compliance department within a financial service provider may need to assess the effectiveness of a new financial crime risk scenario. This implies creating new detection logic, not only adjusting existing thresholds, and it means configuring thresholds, weights, filters, velocity windows, scoring impact and escalation outcomes differently by customer segment, product and jurisdiction.

A starting library of typology rules covering structuring, smurfing, money mule activity, corridor risk and beneficiary risk gives the programme working coverage from deployment, which is then tuned to the institution's own risk profile. However, adaptability at the end of Transaction Monitoring solution may be required which is possible only with solution's ability to detect multiple data points and analyze them to link them to those financial crime scenarios.

Rules that cannot be tested before they generate live work

A rule that cannot be tested against the institution's own historical transaction data before activation is calibrated by estimate. Alert volume and detection rate are discovered only once the rule is live and generating work, and the tuning cycle happens in production.

Backtesting changes both positions at once. The compliance team knows what a scenario will produce before it produces it, and the calibration decision carries documented support. Rule versioning completes the picture, so the version of the logic that fired on a given transaction remains identifiable years later.



Customer Risk that Doesn't Change after Updated Transaction Risk

Customer due diligence establishes a risk position at a single point in time. Transaction monitoring then operates against that position for the life of the relationship. The two are expected to stay connected, with monitoring informing the customer risk assessment and the risk assessment informing what monitoring looks for.

— FIGURE 11

Customer risk feedback loop



MARKED AT THE TWO POINTS WHERE THE LOOP COMMONLY BREAKS

Two failures account for most of the gap, and they are opposites. In the first, monitoring identifies a material change in behaviour and the alert is investigated and closed. But newly identified risk may not be used to update the customer's risk profile. In the second, customer risk changes through periodic review, a screening hit or an ownership update, and the detection logic applied to that customer remains unchanged. The customer is reclassified on paper while monitoring continues against the original profile.

Where Compliance Officers Face Challenges with Transaction Monitoring Solutions

The limitations below recur across deployed transaction monitoring platforms. Which apply to a given institution depends on the platform in use and how it has been configured.

— FIGURE 12

Where traditional TM falls behind

01

Static rules

02

Delayed adaptation

03

Detection gaps

04

False positives

05

Alert fatigue

06

Investigation workload

WORKLOAD CONSTRAINS THE CAPACITY TO CHANGE THE RULES

Detection logic the compliance team cannot change

Many transaction monitoring solutions are rigid. Adjusting a transaction threshold is simple, but configuring a new risk scenario sits with the vendor and moves at the pace of a release schedule. Where the platform offers no library of pre-built typology rules, the compliance team writes every scenario from nothing, and the institution remains accountable for detection coverage it has no practical means to change.

Capacity that doesn't scale with risk exposure

Transaction monitoring complexity grows in several dimensions alongside transaction volume. As an institution adds customers, products, jurisdictions and channels, it also adds scenarios, historical data, alerts and regulatory obligations. A platform adequate at one scale can become the constraint at another, not because throughput fails but because scenarios requiring tuning, alerts requiring disposition and jurisdictional requirements requiring evidence all rise together. The compliance function absorbs that growth, and the operating cost of monitoring rises faster than the business it supports.

No time to decide before an instant payment settles

Traditional transaction monitoring was built for slower settlement, where payments could be held or reviewed before completion. Instant payment rails remove that buffer. Under Regulation (EU) 2024/886, euro instant credit transfers settle within 10 seconds, 24/7, leaving very little time to evaluate customer history, beneficiary context and behavioural risk before funds move.

10s

Under Regulation (EU) 2024/886, euro instant credit transfers settle **within 10 seconds, 24/7**, leaving very little time to evaluate customer history, beneficiary context and behavioural risk before funds move.

That changes the role of monitoring. Controls that depend on post-transaction review or incomplete data are less effective when settlement is immediate and funds may not be recoverable. Real-time decisioning therefore requires the relevant customer and transaction context to be available before execution.

The Regulation also shifts sanctions controls away from screening every individual instant payment. Article 5d requires payment service providers to check at least daily whether users are subject to EU targeted financial restrictive measures, and immediately when those measures change. For instant payments, monitoring architecture therefore has to reflect the control point defined by the payment rail rather than apply a legacy per-transaction model unchanged. ^[17]

Transaction data assessed without context from identity data

Monitoring is materially more useful when the identity and risk context established at onboarding stays connected to later activity. Each transaction can then be assessed not only by amount, timing or channel, but against the verified customer's KYC outcome, AML screening status, risk rating, expected behaviour, relationships and subsequent changes. This becomes more necessary still when the same tool is used not only to monitor transactions but also to detect fraud.

The FCA's January 2025 review supports the principle. Although it focused on wholesale brokers, the FCA said its findings should be considered across wider markets and business models. It found that monitoring transactions in isolation did not regularly identify suspicious activity, because individual transactions may not appear unusual on their own. Alerts should be considered alongside KYC information, intelligence-led analysis, hidden or linked relationships, changes in ultimate beneficial ownership and other relevant information. The FCA also observed that many firms were not using customer risk ratings, expected behaviour, customer activity, jurisdiction risk or wider business and market risk when configuring and maintaining monitoring frameworks. ^[18]

Lower Alert Volume that Misses the Risk

Where every alert enters a single flat queue, the alert carrying genuinely new risk sits alongside the fifth repetition of a pattern already cleared four times. Analysts work in arrival order, and MLRO attention goes to alerts that never required senior review. A lower alert volume may also not translate to effective monitoring, because where a missing data point returns a low-risk result rather than a not assessable flag, the count falls while the risk goes unevaluated.

No record of how a monitoring decision was reached

Where a monitoring programme cannot evidence how it operated, the deficiency surfaces at examination rather than in daily operations. Four gaps account for most of it.

01 **Unversioned configuration and unattributed actions**

The institution cannot state which rule version fired on a given transaction, who approved that rule, or why the case closed as it did.

02 **Reporting deadlines that vary by jurisdiction**

In the United States, a suspicious activity report is generally due within 30 calendar days of initial detection of facts that may constitute a basis for filing, extending to 60 days where no suspect can initially be identified. In the United Kingdom, a report must be made as soon as practicable once the statutory reporting conditions are met. Across the European Union, obliged entities must promptly report relevant suspicions to the national Financial Intelligence Unit. The deadlines are not equivalent, and a multi-jurisdictional institution has to satisfy each on its own terms.

03 **Recordkeeping across jurisdictions**

Five-year retention periods are common across major AML regimes, though the exact records required, the circumstances in which the period extends and the expectations around evidencing decisions all vary by jurisdiction. Rule versioning, decision rationale and auditability are best treated as governance expectations that support any of these regimes rather than as an identical requirement imposed by all of them.

04 **Audit trails that break at the reporting handover**

Where case evidence is exported and re-entered into an FIU portal, each manual handoff between monitoring, case management and reporting creates reconciliation work, introduces the possibility of processing delay and weakens continuity in the audit trail from transaction to filed report.

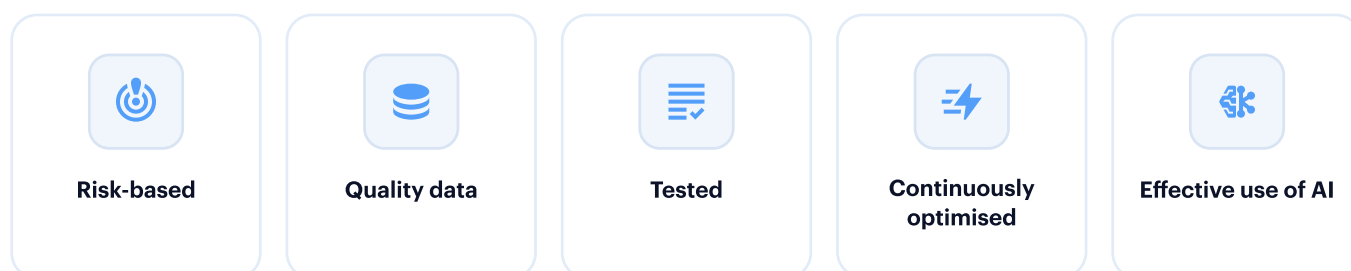
How Financial Regulators Expect Transaction Monitoring Solutions to Operate

Supervisory guidance increasingly focuses not only on whether transaction monitoring is in place, but on how effectively it is designed, tested, calibrated and kept aligned with changing financial-crime risk.

Hong Kong: five principles for effective monitoring

Hong Kong

The HKMA's April 2024 thematic review examined the end-to-end design, implementation and optimisation of transaction monitoring systems, covering governance and oversight, data quality, detection scenarios, threshold setting, periodic review. The crucial aspect is regarding the use of effective AI in Transaction Monitoring Solution. Its observations distill into five practical principles for assessing whether monitoring remains aligned with an institution's changing ML/TF risk.



- **Risk-based.** Detection scenarios should reflect the institution's ML/TF risks, business scope, customer base and transaction patterns, rather than relying on a uniform set of rules and thresholds.
- **Quality data.** The data supporting monitoring should be complete, accurate and correctly mapped, so scenarios operate on the information they were designed to assess.
- **Tested.** Detection scenarios, thresholds and models should be tested and validated before and during use, so institutions understand whether they identify the intended activity and what alert outcomes they produce.
- **Continuously optimised.** Monitoring should be periodically reviewed, calibrated and optimised as customer behaviour, products, risks and financial crime typologies evolve.
- **Effective use of AI.** AI should be applied where it improves the effectiveness or efficiency of monitoring, supported by appropriate governance, data and oversight, rather than treated as an objective in itself. ^[19]

European Banking Authority: five expectations for effective monitoring

European Banking Authority

The EBA's Guidelines on policies and procedures in relation to compliance management and the role and responsibilities of the AML/CFT compliance officer under Article 8 and Chapter VI of Directive (EU) 2015/849, together with its Guidelines on ML/TF risk factors (EBA/GL/2021/02, amended by EBA/GL/2023/03), set expectations for how firms should design, operate and maintain effective transaction-monitoring frameworks. The EBA focuses on risk-sensitive monitoring, customer context, detection effectiveness, proportionality of controls and ongoing system improvement.

These expectations can be summarised into five practical principles:

- **Risk-based monitoring.** Transaction monitoring should be proportionate to the institution's ML/TF exposure. Firms should determine the frequency and intensity of monitoring based on factors including their business model, customer base, products, services and risk profile, rather than applying the same approach across all activity.
- **Customer-contextual detection.** Monitoring should assess whether transactions are consistent with the customer's known profile, financial situation and expected behaviour. Firms should use relevant customer information to identify unusual activity and changes in risk.
- **Effective scenario and pattern detection.** Monitoring systems should be capable of identifying unusual transactions and transaction patterns. Firms should determine which transactions require real-time monitoring and which can be reviewed ex-post, including identifying high-risk factors or combinations of factors that warrant enhanced monitoring.
- **Appropriate automation and system calibration.** Firms should determine whether manual or automated monitoring is appropriate based on their size, complexity and transaction volumes. Where automated systems are used, they should be appropriately calibrated and capable of supporting effective risk detection.
- **Continuous testing and improvement.** Firms should regularly review samples of processed transactions, test whether monitoring systems are reliable and appropriately calibrated, and use findings from reviews, emerging risks and new typologies to improve monitoring scenarios and controls. [\[20\]](#)

Building Transaction Monitoring Solutions In-House- What Are Limitations?

Build or buy

The FCA's January 2025 review observed that "some firms are developing in-house 'reg-tech' solutions to align more effectively with their business, products and customer risk profiles." It also identified challenges around transaction visibility, scalability relative to trade volumes and resources, limited MLTM-specific controls and alerts, and false positives that firms must investigate.

WHERE IN-HOUSE TRANSACTION MONITORING CAN BECOME DIFFICULT

- **Limited data breadth.** Internal systems may not have access to the full range of customer, transaction, counterparty, behavioural, device and contextual data needed to detect complex typologies.
- **High engineering dependency.** New rules, data fields, products and risk scenarios can require repeated development work, keeping compliance dependent on engineering capacity.
- **Typology maintenance burden.** Financial-crime scenarios change continuously. Internal teams must research, design, test and update rules as new predicate-offence risks emerge.
- **Scaling complexity.** Growth across customers, transactions, products and jurisdictions increases processing, scenario and investigation requirements at the same time.
- **Fragmented transaction ingestion.** Supporting multiple payment rails, transaction schemas and messaging standards requires ongoing integration and data-normalisation work.
- **Slower customisation.** Where rule changes require development cycles, monitoring may lag behind changes in the institution's risk exposure.
- **Operational burden.** Running TM in-house also means owning alert operations, investigator workflows, rule tuning, data-quality checks, case management, reporting and audit readiness. As volumes and scenarios grow, that workload can expand faster than transaction volume.
- **Governance overhead.** Backtesting, rule versioning, audit trails, explainability and investigation workflows all need to be built and maintained alongside the detection engine.

How to Choose the Right Transaction Monitoring Solution

The data, context and controls behind effective detection

Effective transaction monitoring depends on more than the rules engine itself. Detection quality is shaped by the transaction and customer data available to the platform, the context applied to each risk scenario, the investigation workflow that follows and the evidence retained for regulatory decisions. The criteria below set out what to assess when evaluating a monitoring solution against the institution's own risk exposure.

— FIGURE 14

What effective monitoring needs to ingest, assess and produce

Input

Transaction data

Payment rails, ISO 20022, SWIFT and SEPA, proprietary schemas, Travel Rule data

Input

Customer identity

Verified identity, KYC outcome, screening status, customer risk rating

Input

Contextual data

Beneficiary and counterparty, device and location, merchant attributes

DETECTION LAYER

Monitoring engine

Enriches the transaction after ingestion so each rule can use the data points relevant to the institution's own risk scenario

Output

Investigation

Case context assembled for review and decision

Output

Reporting

Jurisdiction-specific filing and the evidence behind it

CATEGORIES AS SET OUT IN THIS SECTION

The Right Transaction Data and Contextual Signals to Analyse

TRANSACTION AND PAYMENT-MESSAGE INGESTION



Relevant payment rails. The platform should ingest the transaction records and payment rails the institution actually uses, rather than requiring a fixed universal format.



ISO 20022 support. Modern transaction monitoring should support ISO 20022 so structured payment information can be used effectively within detection logic.



SWIFT and SEPA where applicable. Institutions handling cross-border or European payment flows may also require support for infrastructures and schemes such as SWIFT and SEPA.



Proprietary transaction schemas. The platform should also accept custom or proprietary transaction formats used by fintechs, payment service providers, marketplaces and other financial service providers.



Travel Rule data for virtual asset transfers. Where the institution handles virtual asset transfers, the originator and beneficiary information required under the Travel Rule should reach the detection logic alongside the transfer itself, together with counterparty VASP identity and any on-chain attributes carried with the transaction. Transfers involving unhosted wallets arrive without a counterparty institution supplying that information, so the platform has to record what it did not receive rather than assess the transfer as though the data were present.



Risk-based format coverage. The requirement is not to support every payment format universally, but to process the rails, schemes and message standards relevant to the institution's products, markets and risk exposure.

CONTEXTUAL DATA FOR DETECTION



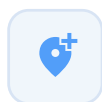
Verified customer identity. Monitoring should have access to verified identity and KYC outcomes so transaction activity is assessed against a known customer profile.



Customer risk and screening context. Customer risk ratings, AML screening status and expected behaviour should be available to the monitoring logic where relevant to the detection scenario.



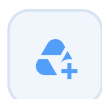
Beneficiary and counterparty data. Beneficiary, counterparty and relationship information can provide context that is not visible from the transaction record alone.



Device and location signals. Device fingerprint, IP and location-related signals can help distinguish expected activity from potentially suspicious behaviour.



Merchant-specific context. For payment service providers and marketplaces, relevant attributes may include merchant classification, merchant category codes and sub-merchant relationships.



Scenario-specific data enrichment. These contextual attributes should enrich the transaction after ingestion, allowing each monitoring rule to use the data points relevant to the institution's specific risk scenario.

Platform Scope, Investigation and Reporting

Data breadth decides what a platform can detect. What happens after detection decides what the compliance function can do with it. The criteria below cover the platform boundaries that determine how much context reaches an analyst, and the workflow that runs between an alert firing and a report reaching the FIU.

COVERAGE ACROSS THE CUSTOMER LIFECYCLE



Identity and monitoring on one platform. Verification at onboarding and monitoring after it ask different questions about the same customer. Where the two sit in separate systems, the monitoring engine scores an account rather than a person, and analysts rebuild identity and screening context by hand during every investigation. A platform carrying the verified identity, KYC outcome, screening status and customer risk rating into transaction scoring removes that rebuild work, along with a vendor boundary that has to be reconciled and evidenced separately at examination.



Fraud and AML assessed in one engine. Money-mule activity and authorised push payment fraud produce signals relevant to both disciplines, as Section 01 sets out. Where fraud and AML run as separate engines, one piece of activity generates two alerts, each carrying part of the picture, and the link between them depends on two teams spotting it independently. Scoring both against the same customer baseline keeps that link inside the system rather than inside a meeting.



One risk position per customer. Ask whether onboarding, screening and monitoring read from and write back to a single customer risk record, or whether each function keeps its own copy. The second arrangement is where the feedback loop in Section 05 usually breaks.

INVESTIGATION AND CASE MANAGEMENT



Case context assembled before review. The work an analyst does before deciding anything is the part that scales badly. Customer history, beneficiary activity, behavioural deviation, linked accounts, screening context and the rule that fired should arrive attached to the case, rather than being collected from four systems every time one opens.



Assignment, collaboration and attribution. Cases move between people. The platform should support assignment, commenting and handover, with every action attributed to a named user and timestamped, because that record is what evidences who decided what.



Tiered review and configurable routing. Routine signals and unusual combinations should not land in the same queue in arrival order. Routing by risk relevance, customer segment, jurisdiction or alert type is what keeps senior review for the cases that need it.



Review controls proportionate to the decision. Four-eyes approval, service level tracking and escalation paths matter most on decisions that carry reporting consequences. Check they can be applied selectively rather than to everything or nothing.

REPORTING, ANALYTICS AND AUDIT EVIDENCE



Filing in the formats each FIU accepts. Reporting obligations differ by jurisdiction in deadline, channel and schema, as Section 04 shows. Where a jurisdiction mandates direct submission in a native format, generating that format from the case is the difference between filing and re-keying.



The evidence package behind a decision. A decision the institution cannot reconstruct is a decision it cannot defend. Transaction records, party data, triggered rules and their versions, the score explanation, analyst actions and timestamps should export together as one record.



Programme-level analytics. Alert volumes, disposition rates, false positive rates, ageing and per-scenario performance are what turn calibration from impression into evidence. Without them, a tuning decision rests on how the queue felt last month.



Visibility of what could not be assessed. A monitoring report that counts only alerts hides the transactions the platform was unable to evaluate. Section 06 covers why a missing data point returning a low-risk result is worse than one flagged as not assessable. Ask how the platform reports data gaps, and whether they surface as a number the MLRO sees.

Deployment, data residency and privacy

Where a platform is offered only as a single hosted model, institutions with data residency obligations are excluded regardless of detection quality. The deployment choice determines where transaction and customer data is processed and stored, which in regulated markets is a legal position rather than a preference, and it is settled before detection capability becomes relevant.

Privacy obligations follow from the same decision. Transaction monitoring processes personal data, including identity attributes, device and location signals and beneficiary detail, so the processing has to sit within the institution's own privacy policy and its lawful basis for handling that data.

Retention periods, access controls and any cross-border transfer arrangements are determined by the jurisdictions the institution operates in, and a monitoring platform has to accommodate those constraints rather than require an exception to them.

AI-Powered Monitoring for Risk Scenario Alignment and Compliance

Shufti's Approach to Risk-Aligned Transaction Monitoring

Shufti translates financial-crime risk into transaction-level detection by connecting verified identity, behavioural and transaction intelligence in one engine. AML and fraud scenarios assess each transaction against the customer and risk context behind it, enabling more precise, explainable compliance decisions. The following maps its approach against the challenges established in this guide.

— FIGURE 15

Challenges established in this guide, and Shufti's approach

CHALLENGE Alert overload	SHUFTI'S APPROACH Risk-aligned prioritisation
CHALLENGE Limited context	SHUFTI'S APPROACH Identity, behaviour & transaction context
CHALLENGE Manual investigation burden	SHUFTI'S APPROACH Risk detection to regulatory decision
CHALLENGE Governance requirements	SHUFTI'S APPROACH Explainable, auditable decisions
CHALLENGE Fraud and AML assessed separately	SHUFTI'S APPROACH AML + fraud, one risk view
CHALLENGE Data residency obligations	SHUFTI'S APPROACH Deployment aligned to regulatory needs

Detection anchored to verified customer context

THE CHALLENGE Transaction monitoring loses precision when transaction data is separated from the customer context established at onboarding. Analysts are then left to reconstruct identity, screening, risk and behavioural context during investigation.

SHUFTI'S APPROACH Shufti connects verified identity, KYC outcomes, AML screening, customer risk, device context and transaction behaviour to the transaction being assessed. Monitoring therefore starts from a known customer and keeps that context attached through detection and investigation.

One transaction, one AML and fraud risk view

THE CHALLENGE Fraud and AML systems can produce separate alerts for the same underlying activity, leaving each team with only part of the risk picture.

SHUFTI'S APPROACH Shufti evaluates AML and fraud signals in the same assessment, including mule activity, structuring, beneficiary risk, device signals and sanctions exposure, so connected risk can move into one investigation rather than separate queues.

The right context for each risk scenario

THE CHALLENGE Real-time monitoring only works when the decision has enough context to distinguish genuine risk from ordinary activity. Faster scoring on limited data simply produces a faster incomplete assessment.

SHUFTI'S APPROACH Shufti provides 24/7 monitoring with 500 ms latency and 1,600+ enriched data points available per transaction. Institutions can configure scenarios around the regulatory, fraud and behavioural signals relevant to their own risk exposure rather than relying on a fixed set of transaction attributes.

24/7

real-time transaction
monitoring

500 ms

latency per call

1,600+

enriched data points available
per transaction

For cross-border activity, Shufti's Transaction Trust Monitoring operates across direct payment flows including SEPA Instant and SWIFT payment messages, using multi-hop analysis to trace relationships between inbound and outbound transfers rather than assessing each payment in isolation.

Turn changing risk into deployable scenarios

THE CHALLENGE When new monitoring scenarios require engineering work or vendor release cycles, detection can fall behind changes in the institution's financial-crime exposure.

SHUFTI'S APPROACH Shufti lets compliance teams configure thresholds, weights, filters, velocity windows, scoring impact and escalation outcomes directly. Teams can start from library of hundreds of pre-built typology rules, create new logic manually or with the AI rule builder, backtest it against historical data and retain version history for governance.

The rules library covers structuring, smurfing, mule activity, corridor risk, beneficiary risk and fraud patterns, so teams adapt monitoring logic as risks evolve without relying on engineering cycles or vendor release timelines.

Beyond thresholds: behavioural and network context

THE CHALLENGE Fixed thresholds and population averages can miss activity that is unusual for one customer or patterns that only become visible across connected accounts.

SHUFTI'S APPROACH Shufti uses a 90-day behavioural baseline to assess transactions against each customer's established activity and applies network analysis to identify coordinated behaviour across linked accounts, devices, IPs, payment identifiers and beneficiaries.

The risk score evolves continuously as behaviour changes, and transaction history supplies the longitudinal view that separates a suspicious sequence from an isolated anomaly.

From Risk Detection to Regulatory Decision

THE CHALLENGE Automating alert generation does not remove the investigation burden if analysts still have to assemble customer, transaction, screening and behavioural context before making a decision.

SHUFTI'S APPROACH Shufti prioritises alerts by risk relevance, routes them to the appropriate review tier and assembles investigation context before the case is opened. Customer history, beneficiary activity, behavioural deviation, linked accounts, screening context and the triggering logic remain available together, reducing the work between detection and regulatory decision.

The analyst finds adverse media, linked accounts, behavioural deviation, the triggering rule and the score explanation together, alongside a plain-English summary, a false positive likelihood and recommended actions. Where the determination is reportable, that same case context carries into a drafted SAR narrative rather than being rewritten by hand.

From composite score to the right reviewer

Scoring and routing

— FIGURE 16

Every transaction scored, every alert routed

Score

Composite 0 to 100
from rules, customer
risk and behavioural
context

Prioritise

Customer memory,
beneficiary history,
velocity, previous
decisions, recurring safe
patterns

Route

Assigned to L1, L2 or
MLRO review and routed
by discipline

TIER ONE

L1

Routine signals logged
without consuming MLRO
attention

TIER TWO

L2

Investigation assembled
before the analyst opens the
case

SENIOR

MLRO

Unusual combinations, with
supporting evidence already
attached

WHICH STEPS RUN IS CONFIGURABLE BY ALERT TYPE, CUSTOMER SEGMENT, JURISDICTION OR RISK POLICY

Scoring, investigation depth and routing can be configured by alert type, customer segment, jurisdiction and risk policy.

Explainable Decisions With Risk-Based Review

THE CHALLENGE A monitoring decision is difficult to defend when the institution cannot show what triggered an alert, what data was available or why the activity was escalated, suppressed or closed.

SHUFTI'S APPROACH Shufti keeps the triggering rules, contributing signals and supporting evidence visible in each case. Missing required data is marked Not Assessable rather than treated as low risk, while suppressed patterns remain recorded and auditable. Final regulatory decisions remain with the analyst and MLRO.

Escalation, filing and audit trail

THE CHALLENGE Manual handovers between monitoring, investigation and reporting create reconciliation work and can weaken the audit trail from transaction to regulatory filing.

SHUFTI'S APPROACH Shufti supports L1, L2 and MLRO escalation, four-eyes review, SLA tracking and action history, with case evidence carried into regulator-ready reporting workflows and retained as an auditable record of how the decision was reached.

Blockchain analytics and Travel Rule compliance

THE CHALLENGE Crypto risk extends beyond the customer account into wallets, blockchain history, counterparty VASPs and unhosted-wallet transfers.

SHUFTI'S APPROACH Shufti brings wallet-level blockchain risk and Travel Rule information into the same monitoring context, including counterparty VASP checks and support for unhosted-wallet workflows.

AI tooling and platform integration

THE CHALLENGE Monitoring configuration can remain locked inside specialist vendor tooling, increasing dependence on support teams for routine changes and questions.

SHUFTI'S APPROACH Shufti supports AI-assisted configuration and external tooling through MCP, helping teams create, understand and manage monitoring logic without relying on support cycles for routine tasks.

Deployment, security and regulatory alignment

THE CHALLENGE Data residency, security and procurement requirements can eliminate a monitoring platform before detection capability is even considered.

SHUFTI'S APPROACH Shufti supports SaaS, private cloud and on-premise deployment, with coverage across 240+ countries and territories and independent audits including SOC 2 Type II, PCI DSS and ISO/IEC 27001:2022.

References

Sources

- 1 Swiss Financial Market Supervisory Authority (FINMA), *Money laundering supervision: findings from the on-site supervisory reviews*, 2024.
- 2 U.S. Department of Justice, *TD Bank Pleads Guilty to Bank Secrecy Act and Money Laundering Conspiracy Violations in \$1.8B Resolution*, press release, 10 October 2024. See also FinCEN, *FinCEN Assesses Record \$1.3 Billion Penalty against TD Bank*, 10 October 2024.
- 3 Financial Conduct Authority, *Payment account providers' systems and controls against money mule activity (multi-firm review)*, 2023.
- 4 Financial Conduct Authority, *Firms' use of the National Fraud Database (NFD) and money mule account detection tools*, January 2025.
- 5 FINTRAC, *Updated Indicators: Laundering of proceeds from human trafficking for sexual exploitation*, Operational Alert FINTRAC-2021-OA001, July 2021.
- 6 FinCEN, *Guidance on Recognizing Activity that May be Associated with Human Smuggling and Human Trafficking*, Financial Red Flags, Advisory FIN-2014-A008, 11 September 2014.
- 7 FinCEN, *Alert on Human Smuggling Along the Southwest Border of the United States*, FIN-2023-Alert001, 13 January 2023.
- 8 FinCEN, *Financial Trend Analysis: Human Smuggling, 2023–2025*, 13 August 2026.
- 9 FinCEN, *Advisory to Financial Institutions on Illicit Financial Schemes and Methods Related to the Trafficking of Fentanyl and Other Synthetic Opioids*, Advisory FIN-2019-A006, 21 August 2019.
- 10 FinCEN, *Supplemental Advisory on the Procurement of Precursor Chemicals and Manufacturing Equipment Used for the Synthesis of Illicit Fentanyl and Other Synthetic Opioids*, Advisory FIN-2024-A002, 20 June 2024.
- 11 FinCEN, *Alert on Prevalent Virtual Currency Investment Scam Commonly Known as "Pig Butchering"*, FIN-2023-Alert005, 8 September 2023.
- 12 FinCEN, *FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts*, Alert, 7 March 2022.
- 13 U.S. Departments of Commerce, the Treasury and Justice, *Tri-Seal Compliance Note: Cracking Down on Third-Party Intermediaries Used to Evade Russia-Related Sanctions and Export Controls*, 2 March 2023.
- 14 FinCEN and U.S. Department of Commerce Bureau of Industry and Security, *Joint Alert: Urging Increased Vigilance for Potential Russian and Belarusian Export Control Evasion Attempts*, FIN-2022-Alert003, 28 June 2022.
- 15 FinCEN and Bureau of Industry and Security, *Supplemental Joint Alert: Urging Continued Vigilance for Potential Russian Export Control Evasion Attempts*, May 2023.
- 16 FinCEN and Bureau of Industry and Security, *Joint Notice: New Reporting Key Term and Red Flags Relating to Global Evasion of U.S. Export Controls*, FIN-2023-NTC2, 6 November 2023. Introduced the SAR key terms FIN-2022-RUSSIABIS and FIN-2023-GLOBALEXPORT.
- 17 Regulation (EU) 2024/886 on instant credit transfers in euro.
- 18 Financial Conduct Authority, *Assessing and reducing the risk of Money Laundering Through the Markets (MLTM)*, January 2025, paragraphs 1.8, 9.13, 11.4 and 11.6–11.7.
- 19 Hong Kong Monetary Authority, *Thematic Review of Transaction Monitoring Systems and Use of Artificial Intelligence*, and accompanying *Insights for Design, Implementation and Optimisation of Transaction Monitoring Systems*, 17 April 2024.
- 20 European Banking Authority, *Guidelines on ML/TF risk factors under Articles 17 and 18(4) of Directive (EU) 2015/849*, EBA/GL/2021/02, amended by EBA/GL/2023/03; Sections 4.69–4.75.



Every transaction scored. Every decision explained.

Bring one of your own risk scenarios. Fraud and AML are assessed together in one engine, configured to your risk exposure rather than a fixed rule set, and we'll walk it through to the point a reportable determination gets made.

[Book a demo](#)

Legal Disclaimer

The information provided here is for general informational purposes only and should not be treated as legal, regulatory, or business advice. Shufti Pro Limited accepts no liability for decisions or actions taken in reliance on this information.

Shufti is based in the United Kingdom and operates offices worldwide.



United States

16200 SW Pacific
Hwy, Suite H PMB
1053,
Tigard, OR



Cyprus

Arch. Makarios III
Avenue 229,
Limassol



Dubai

Unit 507, Level 5,
Gate District
Precinct
Building 03, DIFC,
Dubai



Hong Kong

8 Queen's Road
East, Wan Chai,
Hong Kong



Pakistan

322-G3 Main Blvd,
Johar Town, Lahore,
Pakistan



Singapore

68 Circular Road
#02-01, Singapore



United Kingdom

Office 408,
Coppergate
House, 10 Whites
Row, London E1
7NF

shuftipro.com
sales@shuftipro.com