

AML & TRANSACTION MONITORING SECURITY.

Transaction monitoring watches ongoing flows for patterns — structuring, layering, unusual velocity — that a single-transaction fraud control was never built to see. **But the monitoring system is itself infrastructure, and a rule an insider can quietly disable is a control that was never really there.**

- TRANSACTION MONITORING
- SAR & CTR FILINGS
- RULE INTEGRITY
- STRUCTURING DETECTION

01 THE MECHANISM



Pattern Detection, Not Transaction Blocking

Monitoring watches ongoing flows for structuring, layering across accounts, or velocity unusual for a customer's baseline, **generating alerts rather than blocking individual transactions** in real time.



SARs and CTRs Are Different Systems

A currency transaction report is a bright-line requirement above a dollar threshold; a suspicious activity report is a confidential judgment call — **tipping off the customer is itself a federal crime.**



The Monitoring System Is Itself a Target

Detection rules, thresholds, and alert queues are infrastructure an insider can tamper with — **a disabled rule or a buried alert functions like a disabled control**, even though nothing was technically hacked.

02 THE FLOW

The Governed, Auditable Program

CONTAINED

1

Every change to a detection rule or threshold requires independent approval and is logged, so **a single insider can't quietly suppress alerts** for a specific account.

2

Independent testing periodically validates the monitoring system actually catches what it's supposed to, rather than **assuming the rules still work** as originally designed.

3

Alert queues are resourced to match real volume, so a **true positive doesn't get lost** in an unmanageable backlog.

The Unmonitored Monitoring System

EXPOSED

1

A single employee with unreviewed access quietly adjusts detection thresholds for a specific account, and **no one else is positioned to notice** the change.

2

Alert volume has grown far beyond what the investigation team can review, so **true suspicious activity sits indistinguishable** from thousands of false positives.

3

The program passes a superficial check because the rules exist on paper, but **independent testing never validated** whether they still catch what they're supposed to.

03 CORE PILLARS & COVERAGE

PILLAR	WHAT IT COVERS
Risk-Based Customer Due Diligence	Understanding a customer's expected transaction behavior at onboarding, which anchors what counts as a meaningful deviation later.
Transaction Monitoring & Alerting	Rules and analytics scanning transaction flows for structuring, layering, and velocity patterns, generating alerts for investigator review.
Rule Integrity & Change Control	Independent approval and logging for any change to detection rules or thresholds, so tampering doesn't go unnoticed.
Independent Testing & Audit	Periodic validation that the monitoring program actually catches what it's designed to, distinct from having the rules exist on paper.

04 DETECTION APPROACHES COMPARED

APPROACH	SUFFICIENT ALONE?	WHAT IT MISSES
Rules Deployed With No Change Control or Audit Trail	No	A detection threshold anyone can quietly adjust with no independent review is a control an insider can disable without a trace.
Alert Volume Exceeding Investigation Capacity	No	A queue too large to meaningfully review functions the same as having no monitoring, regardless of how sophisticated the rules are.
Assuming the Program Works Because It Was Built Correctly Once	No	Without independent testing, a monitoring program can develop blind spots or drift for years without anyone noticing.
Treating CTRs and SARs as the Same Requirement	No	A CTR is a bright-line dollar-threshold requirement; a SAR is a confidential, judgment-based filing — confusing the two creates real gaps.
Change-Controlled Rules + Resourced Alert Review + Independent Testing + Confidential SAR Process	Yes	Keeps the detection layer itself trustworthy, not just the policy describing it.

AML & TRANSACTION MONITORING.

DETECT · REPORT · VALIDATE

05 PROGRAM OPERATIONS

A monitoring rule anyone can quietly change without independent review is a control an insider can disable without ever touching a system an outsider would recognize as "hacked."

Alert fatigue isn't just an inefficiency. A queue too large to meaningfully investigate makes a true positive functionally indistinguishable from the noise around it.

Tipping off a customer that a SAR has been filed against them is a federal crime in its own right, independent of whatever underlying activity triggered the filing.

Structuring transactions to stay under the CTR reporting threshold is itself a distinct federal crime, regardless of whether the underlying funds turn out to be legitimate.

06 CONTROL MAPPING

BANK SECRECY ACT (BSA)

The foundational US law requiring financial institutions to maintain records and file reports that assist in detecting and preventing money laundering.

FINCEN

The Treasury bureau that administers the BSA, collects SAR and CTR filings, and issues AML regulations and guidance.

FINCEN'S FIVE PILLARS

Internal controls, independent testing, a designated compliance officer, ongoing training, and risk-based customer due diligence.

AML ACT OF 2020

Amended the BSA to formally add customer due diligence as an explicit program pillar and expanded FinCEN's regulatory authority.

07 WHAT THIS DOES NOT SOLVE

Preventing the Underlying Crime

Monitoring detects and reports patterns after the fact; it **doesn't prevent the predicate criminal activity** generating the illicit funds.

Real-Time Transaction Blocking

Most AML monitoring generates alerts for investigation, not automatic blocks, so a **flagged transaction may still complete** before anyone reviews it.

Sophisticated, Patient Layering

A patient launderer who structures transactions well under thresholds and disperses funds across many accounts can **still evade pattern-based detection**.

Cross-Institution Visibility

A bank's monitoring system sees its own flows; it has **no native visibility into how funds move** once they leave for another institution entirely.

08 MYTHS VS. REALITY

MYTH	REALITY
"AML monitoring blocks suspicious transactions in real time."	Most monitoring systems generate alerts for investigator review after the fact; they don't automatically block a transaction the way a fraud-prevention control might.
MYTH	REALITY
"A SAR filing and a CTR filing serve the same purpose."	A CTR is a bright-line requirement triggered automatically above a dollar threshold; a SAR is a confidential, judgment-based filing tied to suspicion of illicit activity.
MYTH	REALITY
"As long as we stay under \$10,000, we avoid reporting entirely."	Deliberately structuring transactions to stay under the CTR threshold is itself a distinct federal crime , independent of the underlying funds.
MYTH	REALITY
"Once the monitoring rules are built, the program is compliant."	Independent testing exists specifically because rules can drift out of effectiveness or develop blind spots for years without validation.
MYTH	REALITY
"A large alert volume just means the system is working hard."	A queue too large for investigators to meaningfully review functions the same as having no effective detection at all.

09 SPEAK THE PROGRAM — KEY TERMS

SUSPICIOUS ACTIVITY REPORT (SAR)

A confidential filing to FinCEN reporting activity that may indicate illicit activity; **tipping off the customer is a federal crime**.

CURRENCY TRANSACTION REPORT (CTR)

A mandatory filing for cash transactions exceeding \$10,000, **required regardless of suspicion**.

STRUCTURING

Deliberately breaking up transactions to stay under the CTR reporting threshold, **itself a distinct federal crime**.

LAYERING

Moving illicit funds rapidly through multiple accounts or institutions to obscure origin, **a pattern monitoring is specifically designed to detect**.

ENHANCED DUE DILIGENCE (EDD)

Additional scrutiny applied to higher-risk customers, such as **politically exposed persons or cash-intensive businesses**.

KNOW YOUR CUSTOMER (KYC)

Verifying customer identity and expected transaction behavior at onboarding, **anchoring what later counts as a meaningful deviation**.