SUTHERLAND®

FRAML 2.0

A CxO Playbook for Unifying Fraud & AML in the Age of AI

How Modern Financial Institutions Can Fight Financial Crime in 2025 and Beyond...

Table of Contents

The Financial Crime Surge:
An Escalating Battlefield

Financial institutions today stand at a pivotal inflection point. Financial crime has not only grown in volume, but in complexity, sophistication, and cost. Fraud, money laundering and cybercrime have converged in ways that challenge traditional detection models and overwhelm operations.

This is no longer about isolated risk events. Sophisticated actors are blending fraud tactics—such as mule accounts, synthetic IDs, and ATO—with money laundering schemes across multiple channels and geographies. Yet, most institutions still operate with fragmented fraud and AML programs.

"The real threat isn't just more fraud. It's the inability of siloed systems to see the full picture."

Financial Crime at a Glance (2024 vs 2021)

$5.8B *reported fraud losses in the US in 2021*
$10.5B *in 2024*[1]

41% *YoY rise in bank fraud incidents*[2]

85% *of all fraud now involves synthetic identities*[3]

22% *of US adults report ATO (Account Takeover), average loss:* ***$12,000***

1 FTC, Bloomberg 2 PYMNTS 3 McKinsey

Fraud isn’t **“One Size Fits All”**

Fraud typologies evolve differently across sectors.
What plagues a global retail bank may look completely different for a digital payments platform or a high-velocity BNPL fintech. Payment processors often face refund abuse and merchant acquirer fraud, while banks are dealing with ATO, check fraud & money mule networks. The risk surface is as unique as the business model.

A unified fraud and AML strategy must therefore be context-aware — built on flexible models, dynamic rulesets & behavioral analytics tailored to each vertical’s exposure.

To truly unify FRAML, institutions must first localize fraud — by sub-sector, channel, and customer journey.

	Common Fraud Types	Examples
Retail Banks	ATO, Check fraud, Credential stuffing	Credential-stuffed ATO during stimulus payments
Neobanks / Challenger Banks	Synthetic IDs, KYC bypass, money mules	Onboarding fraud via fake documents
Payments / PSPs	Merchant fraud, refund abuse, APP	Fake merchant bust-outs exploiting high STP
BNPL / Lending	Application fraud, synthetic identity fraud, bust-out	New account fraud using social security fabrication

Case in Point:
Fraud threats across customer journey

Fraud isn't a single event. It's a series of interlinked manipulations that unfold across the entire customer lifecycle — from onboarding synthetic identities to exploiting dormant accounts or engineering social access to credentials. As illustrated, each touchpoint is a vulnerability, and no team can handle them in isolation.

The future of fraud detection lies in stitching together fragmented moments into a single, intelligent risk storyline.

1 Customer Onboarding	2 Account Access	3 Account Self Management	4 Account Utilization	5 Account Expansion
AREAS OF CONCERN				
New account fraud	Account takeover		Account takeover	Flat mule accounts
Synthetic ID	Scams		Scams	Payment data
Bots	Social engineering		Identity theft	Beneficiary data
Recognize trusted customers	Bots		Social engineering	Continuous authentication
Facilitate NAO	Recognize returning customers		Funds withdrawals	Reduce additional barriers
Speed up onboarding	Risk-based authentication to limit customer impact		Seamless checkout payment	
			Reduced step-ups: risk based authentication to limit customer impact	

Legacy FinCrime Compliance Solutions are no longer ‘Fit for Purpose’ and are failing modern compliance needs

Compliance as a Barrier to Growth	High Abandonment Rates Due To Needless Manual Alert Remediation	High False/Positive Rates Impacts **STP Rates** Stifling Global Growth	High Customer Expectation Amplify Impact of **Transaction Delay**
Increasing Cost of Financial Crime Compliance	**14% YoY Increase** In Cost Of Financial Crime Compliance	N**umerous wasted hours** manually remediating ‘False Positive’ Alerts	**Growing Cost of Fraud** Reimbursement and Customer Support
Increasing Pressure of Regulatory Oversight & Fraud	In 2023 **$6.2B In Fines** Were Handed Down	**Glencore, Entain & BAT** all fined >$500M last year	**Over 13,000+ new sanctions** restrictions imposed since 2022

Operational Fragmentation is **The Real Enemy!**

Despite years of investment, fraud and AML operations are still structured in silos:

- Separate teams, tech stacks, data models, case systems
- No shared risk signals, watchlists, or behavioral insights
- Overlapping false positives, duplicated investigations

These disjointed approaches lead to inefficiencies, audit vulnerabilities and missed signals.

A fraud alert dismissed in isolation may have triggered a SAR if linked to broader laundering behavior. Conversely, AML alerts often lack the behavioral context fraud teams can provide.

Common Gaps Between Fraud and AML Ops

Area	Fraud	AML
Identity Verification	Real-time risk scoring	Document-heavy KYC/CDD
Alert Thresholds	Velocity-based	Volume/value-based
Investigation	Transaction-centric	Customer-centric
Case Tools	Workflow-driven	Compliance-logged
Feedback Loops	Limited model learning	Often manual

AML in Crisis — **Complexity Outpacing Control**

Top AML weaknesses

1. **High false positives** due to outdated rules
2. **SAR** narrative quality & audit **inconsistency**
3. **Poor linkage** between TM and real-world behavior

> ***AML is still stuck in 2010 — spreadsheets, scripts & slow case systems. AI without context is just noise.***

Manual SAR narratives, siloed data, and limited behavioral signals have made AML detection not only slow but alarmingly ineffective. The need of the hour is a shift from static, compliance-driven routines to an intelligent AML lifecycle — where monitoring, investigation & reporting are seamlessly integrated with AI-guided decisioning and real-time context.

The Modern AML Lifecycle

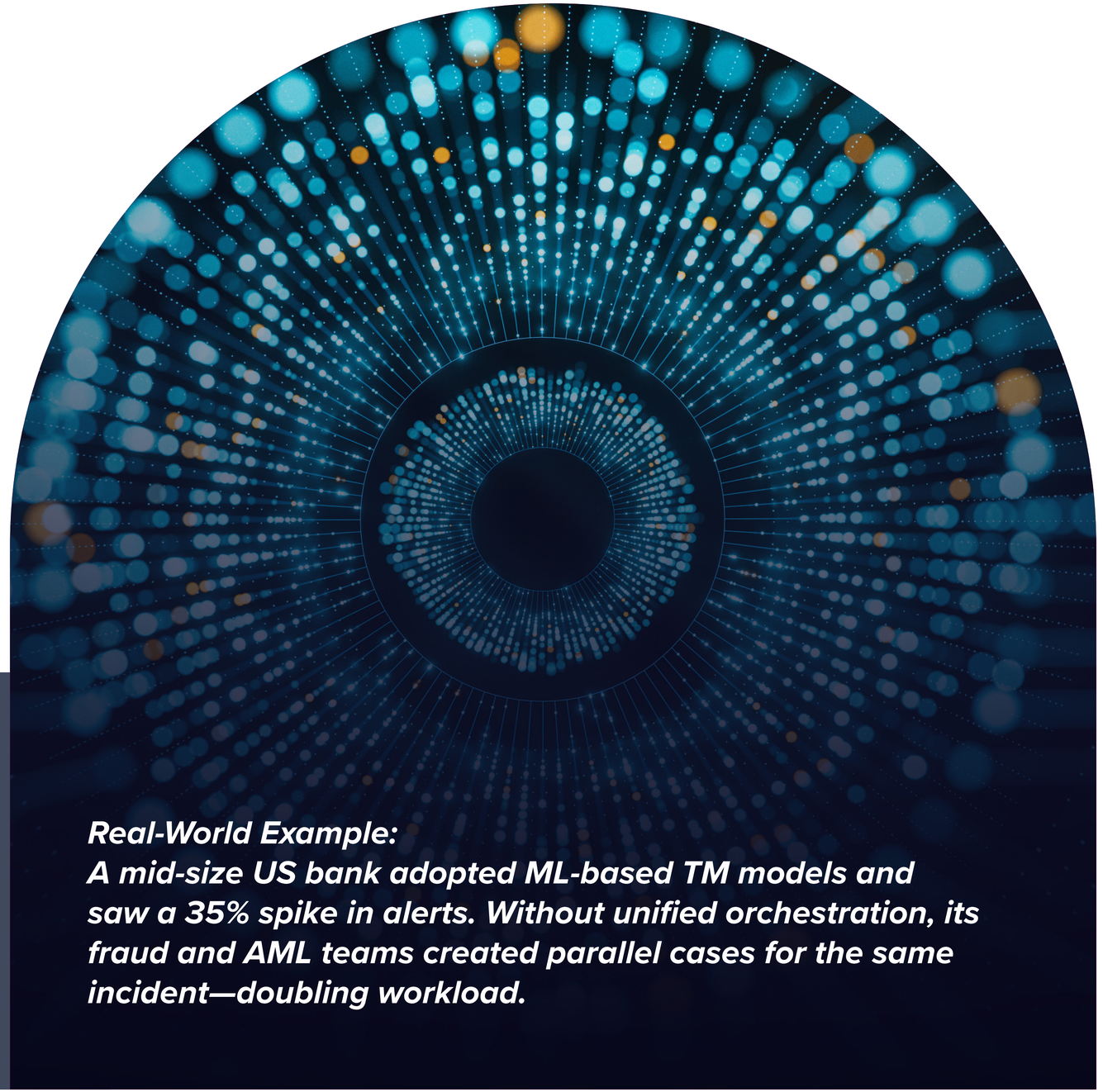
The modern AML lifecycle leverages integrated monitoring, contextual investigation, and AI-assisted reporting to respond swiftly to evolving threats. It enables a seamless flow of risk intelligence across teams, reducing blind spots and improving regulatory confidence.

The **AI** Paradox:
Smarter Tools, Harder Decisions

AI has revolutionized detection. But it has also raised the stakes:

- AI models surface more nuanced anomalies—but generate more alerts.
- GenAI speeds SAR drafting and case resolution—but amplifies model governance risk.
- LLMs can simulate customer behavior—but may mislead under false inputs.

The promise of AI is real. But without integrated data, context and workflows, AI creates complexity faster than institutions can absorb it.



"The challenge isn't building better models. It's orchestrating them across risk domains."

Real-World Example:
A mid-size US bank adopted ML-based TM models and saw a 35% spike in alerts. Without unified orchestration, its fraud and AML teams created parallel cases for the same incident—doubling workload.

The Case for FRAML: Strategic Unification

FRAML 2.0 Framework

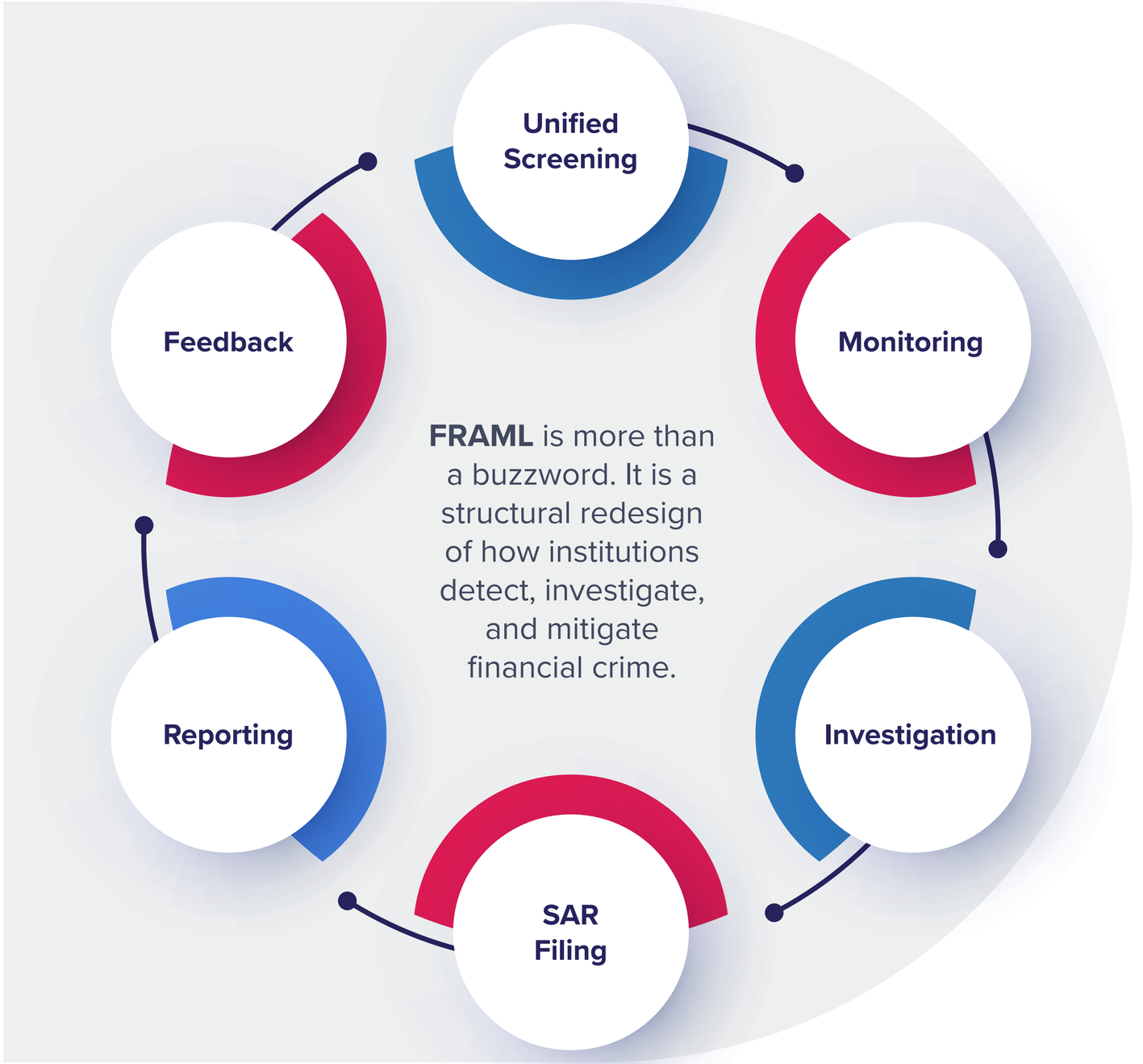
Single Alert Pipeline:
Fraud and AML alerts share a common queue with domain-specific routing.

Behavioral + Transactional Fusion:
Merge fraud behavior analytics with AML transaction typologies.

Case Convergence:
One case, one investigator, full 360° view across fraud + AML dimensions.

Agentic AI Layer:
Autonomous agents prioritize, escalate, and guide investigations using real-time context.

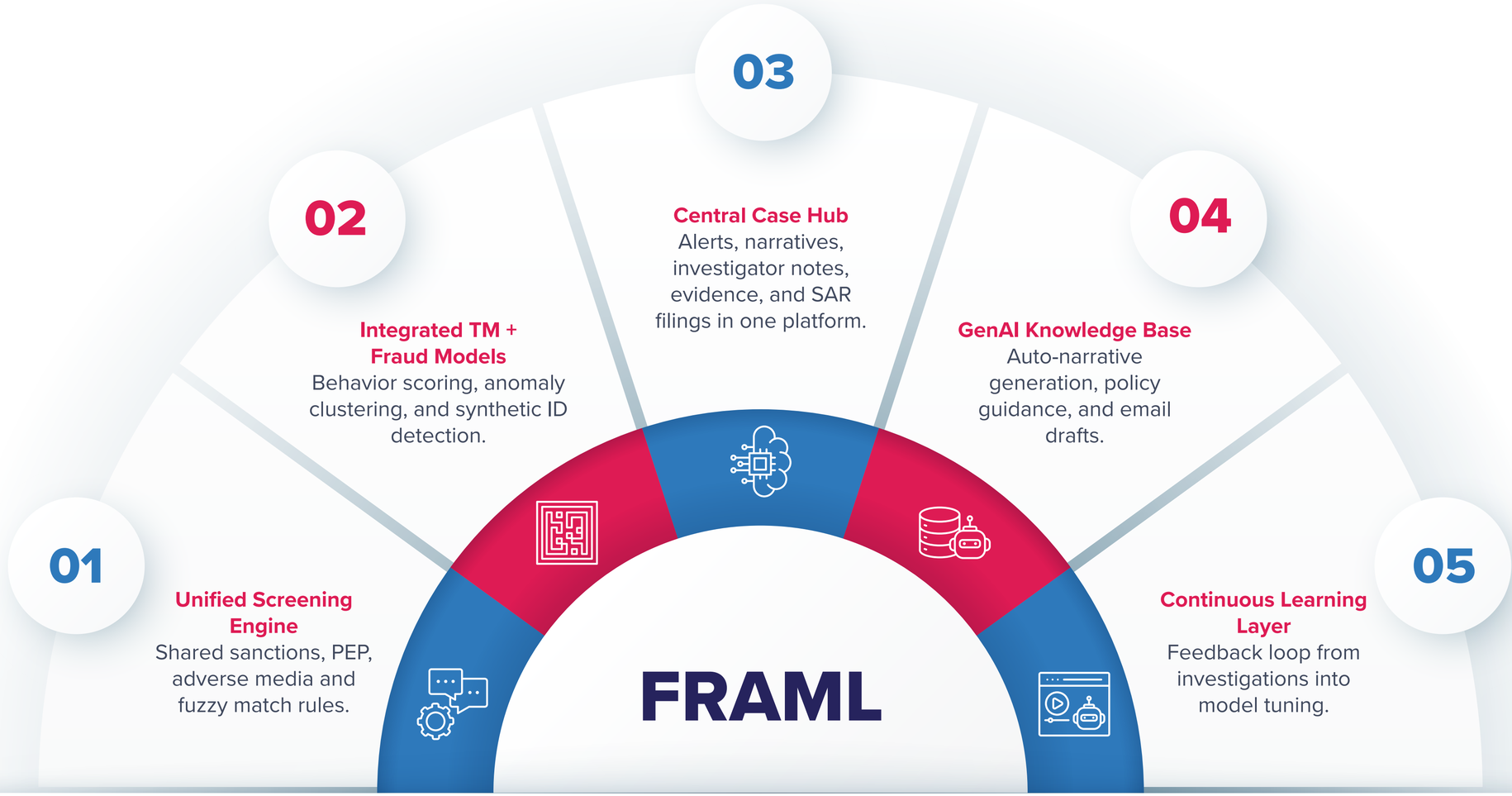
Composable Ops:
Modular services for screening, KYC, TM, SAR, and analytics built on shared APIs.



FRAML in Practice:
A Modular Operating Model

A well-architected FRAML model is not monolithic. It is Composable, Intelligent & Human-centered.

Critical Modules



FRAML **2.0**

CxO Tearsheet

5 Step Playbook for **FinCrime Ops Reinvention**

Modernizing financial crime operations isn't just about adopting AI — it's about reengineering how fraud and AML are managed across teams, systems, and intelligence layers. This 5-step playbook offers a structured path forward.

1. **Conduct enterprise-wide risk map aligning AML & fraud events**
2. **Select unified case management platform**
3. **Form cross-functional convergence team**
4. **Train for hybrid investigator roles (AML + Fraud)**
5. **Implement feedback-based model tuning layer**

What looks "Good" in 2027

Capability	Traditional State	FRAML 2.0 Target
Alert Triage	Manual queues	AI-routed, context-rich
Investigation	Dual tracks	Single case file
Customer Experience	Repetitive KYC	Frictionless, one-touch
SAR Narrative	Manual drafting	AI-assisted + reviewer sign-off
Audit Trail	Fragmented	Unified, auto-logged
Operating Model	Tool-driven	Modular BPaaS + SMEs

Actions for Risk & Fraud Leaders Tools, Harder Decisions

Success Story: *Global Blockchain FI Implemented unified onboarding and screening workflows with AI-led risk scoring.*

Outcome: *80% faster onboarding, 50% fewer escalations, 100% audit-ready trail.*

STRATEGIC ALIGNMENT

- Mandate convergence of fraud and AML within 12-18 months
- Include FRAML in enterprise risk and compliance roadmap

PEOPLE & CULTURE

- Train SMEs in cross-domain typologies
- Introduce GenAI co-pilots with audit traceability

TECHNOLOGY & INTEGRATION

- Modernize alert pipeline with AI orchestration layer
- Consolidate case tools; integrate GenAI for SAR workflows

MEASUREMENT & FEEDBACK

- Track efficiency KPIs: false positives, alert remediation times, SAR yields
- Monitor GenAI impact: productivity, consistency, regulatory feedback

Assess Your FRAML Maturity

Where does your institution stand on the FRAML maturity? Whether you're just starting to align fraud and AML alerts or already piloting AI-assisted case workflows, benchmarking is the first step toward strategic advancement. Use this matrix to self-assess & plot your path ahead!

Dimension	Level 1	Level 2	Level 3	Level 4
Data Sharing	Separate	Manual Extracts	API-linked	Unified Data Fabric
Case Workflow	Manual	Semi-automated	Unified With Audit Trail	Orchestrated AI Co-pilot
Alert Accuracy	<20% Precision	40–50% Precision	Smart Prioritization	AI-led Resolution
Investigator Roles	Fully Siloed	Some Cross-training	Hybrid Risk Roles	Agent-assisted Pods
Regulatory Readiness	Manual Logs	Batch SARs	Real-time Reports	Auto-narrative, Auditor Ready

Institutions that approach FRAML reinvention as a business transformation — not just a tooling upgrade — will be better prepared for what's next.

Sutherland

FRAML

Sutherland FRAML

Enabling FCC domain expertise & services at scale across the value chain

25+ Clients
in FCC & Fraud

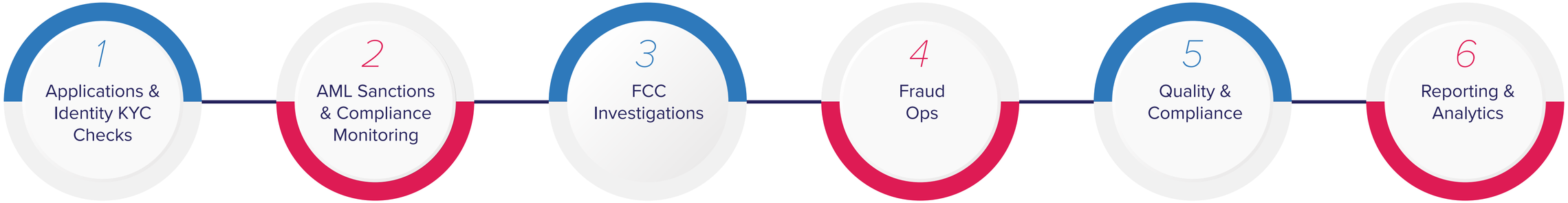
2,400+ SMEs
in Financial Crime, Fraud & Risk Ops

~30% Benefits
(Reduction in False Positives, TCO Reduction)

20%+
CSAT Improvement

Expertise Across
Cards, Payments, BNPL, Deposits, Travel, Retail, Ecommerce

Services Overview



Applications & Identity

- Identity proofing and KYC validation
- Fraudulent applications review and flagging
- ID document verification
- Video-enabled KYC Verification and liveness verification

Compliance & Fraud Detection

- CDD, EDD L1/L2 alert remediations
- Sanctions screening
- Transaction monitoring & real-time data enrichment
- Watch list & adverse media screening
- Policy review & enforcement

Investigations

- Fraud transaction analysis, resolution & recovery
- Fraud prioritization (likelihood, severity) exceptions & case management
- Transaction anomalies and suspicious activities
- Forensic audits & analysis
- SAR preparation

Resolution and Reporting

- Disputes logging and investigation
- Chargeback analysis and resolutions
- Database enrichment and maintenance
- Compliance reporting

Sutherland FRAML | Digital Accelerators

SUTHERLAND® FinTelligent

Agentic AI Automation

Sutherland FinTelligent supports FRAML by using automation and AI to detect fraud and AML risks faster and more accurately by continuously improving risk models.

SUTHERLAND® ID Scan

ML Based Doc Verification

Sutherland's ID Scan uses AI to quickly verify IDs, detect fakes, and enable secure onboarding.

SUTHERLAND HelpTree®

GenAI Knowledgebase

HelpTree is a GenAI-powered tool that provides real-time, context-aware guidance and email drafts to support agents during live workflows.

SUTHERLAND® Data Analytics

Advanced AI/ML Models

Sutherland uses advanced AI/ML in data analytics to find patterns, predict outcomes, and improve decisions—boosting customer experience, efficiency, and fraud detection.

SUTHERLAND Sentinel AI®

Data Security & PII Handling

Sutherland Sentinel AI® protects data in real-time using AI to detect, mask, and secure sensitive information with redaction, encryption, and access controls.

Sutherland Client Outcomes

60%
false positive reduction

50%
alert handling time reduction

30%
drop in fraud TCO

Whether you are building your first integrated compliance stack or modernizing a legacy risk operation, Sutherland offers the architecture, expertise, and results to deliver a future-ready FRAML program.

Artificial Intelligence. Automation. Cloud Engineering. Advanced Analytics. For Enterprises, these are key factors of success. For us, they're our core expertise.

We work with global iconic brands. We bring them a unique value proposition through market-leading technologies and business process excellence. At the heart of it all is Digital Engineering – the foundation that powers rapid innovation and scalable business transformation.

We've created over 200 unique inventions under several patents across AI and other emerging technologies. Leveraging our advanced products and platforms, we drive digital transformation at scale, optimize critical business operations, reinvent experiences and pioneer new solutions, all provided through a seamless "as-a-service" model.

For each company, we provide new keys for their businesses, the people they work with, and the customers they serve. With proven strategies and agile execution, we don't just enable change – we engineer digital outcomes.

SUTHERLAND®
digital outcomes.

sutherlandglobal.com

