VERISTACK INC.

Sentinel

AI-Powered AML Compliance.
Built for Regulators. Ready Today.

Product Overview · Confidential

June 2026

sentinel.veristack.ca

VeriStack Inc. · veristack.ca

Who Sentinel Is For

Sentinel is built for the compliance leaders who carry personal regulatory liability and the institutions that cannot afford a multi-year, multi-million-dollar platform rollout.

Your institution, if you are:

- A commercial bank, microfinance bank, fintech, payment service provider (PSP), or mobile money operator (MMO) operating under CBN supervision
- An institution processing anywhere from thousands to millions of transactions per month
- A team that needs to submit a credible AML automation roadmap to the regulator by June 2026

Your role, if you are:

- A Chief Compliance Officer or MLRO (Money Laundering Reporting Officer) who signs off on AML controls and answers to the board and the regulator
- A Head of Compliance managing a small team drowning in manual reviews
- A Head of Risk or COO weighing the cost of a fine against the cost of a system

If a regulator can hold you personally accountable for a missed suspicious transaction, Sentinel is built for you.

The Regulatory Moment

In March 2026, the Central Bank of Nigeria issued a directive that changed the compliance landscape overnight: **automate your AML systems or face consequences.**

- Fintechs, PSPs, and MMOs have 24 months to comply
- Commercial and microfinance banks have 18 months
- Every institution must submit a compliance roadmap by June 2026

But this is not just a Nigerian story. OSFI in Canada, the FCA in the UK, and FinCEN in the US are all moving toward the same expectation: AI in your compliance stack must be auditable, explainable, and governed.

The clock is running. For everyone.

What Compliance Looks Like Today

Most compliance teams still operate like this:

- A compliance officer manually reviews flagged transactions in spreadsheets or basic dashboards
- Sanctions screening happens in one system, KYC in another, and case files in a third
- New customers are onboarded with minimal pre-screening and flagged only after suspicious activity
- When something suspicious is found, the SAR is drafted by hand and filed days later
- When a regulator asks "why was this customer flagged?" or "why was this one missed?", the answer takes hours to piece together
- Dormant accounts reactivate with large transfers, and nobody notices for weeks

This approach is slow, fragmented, and impossible to defend in a modern audit.

What it costs you:

- Analysts spend the majority of their time clearing false positives instead of investigating real risk
- Every manual SAR is hours of analyst time, and late filings carry regulatory penalties
- A single missed sanctions hit can mean fines, license risk, and personal liability for the MLRO
- When the regulator arrives, reconstructing a decision chain by hand can take days you do not have

What Sentinel Changes

Sentinel is built to move your team from reactive, manual, and indefensible to proactive, automated, and audit-ready.

TODAY (MANUAL)	WITH SENTINEL
Analysts buried in false positives	Confidence-gated triage routes only genuine uncertainty to humans, so analysts focus on real risk
SARs drafted by hand over hours or days	SARs auto-drafted in NFIU-ready format with evidence attached, ready for human approval in minutes
"Why was this flagged?" takes hours to answer	One click returns the full decision chain with timestamps, confidence scores, and reviewer names
Screening happens once, at onboarding	Continuous re-screening catches a customer who becomes sanctioned months after joining
Fragmented tools, no single source of truth	One platform covering onboarding through monitoring through reporting
Audit readiness is a fire drill	Audit readiness is the default state, every decision logged permanently

The business case in one line: Sentinel reduces the analyst hours spent per case, shortens time-to-file on SARs, and makes the regulator question a same-day answer instead of a multi-day scramble.

> Note: Quantified benchmarks (false-positive reduction, hours saved per case) are measured during your proof of concept against your own historical data, so the numbers are yours, not ours.

The Full AML Lifecycle in One System

Sentinel is not a monitoring tool. It is a **complete AML compliance platform** that covers the entire customer lifecycle: from the moment a customer applies to open an account, through every transaction they make, and across every watchlist update for as long as they remain a customer.

Two pipelines. Seven agents. One governance engine.

Pipeline 1: Customer Onboarding Before a customer can transact, Agent 0 screens them against every watchlist. Sanctions match? Blocked automatically. PEP (Politically Exposed Person) match? Escalated to the Head of Compliance for documented approval. Clean? Onboarded with a risk tier and entered into continuous monitoring.

Pipeline 2: Transaction Monitoring When a transaction enters the system, six specialized agents process it:

1. **Transaction Monitor:** Checks regulatory thresholds, velocity bursts, dormant account reactivation, structuring patterns, and time-of-day anomalies
2. **KYC Verifier:** Confirms identity against BVN (Bank Verification Number) and NIN (National Identification Number) records, flags PEPs, assigns risk tiers
3. **Watchlist Screener:** Screens against 19,000+ live entries from OFAC, UN, and Nigerian domestic lists
4. **Pattern Analyzer:** Analyzes 90 days of behavioral data for layering, round-tripping, and geographic anomalies
5. **SAR Generator:** Drafts Suspicious Activity Reports in NFIU-ready format with all evidence packaged
6. **Case Manager:** Opens investigation cases, tracks deadlines, manages escalation workflows

All seven agents process a transaction in **under one second.**

The Governance Engine

Speed means nothing without control. Sentinel's governance engine enforces **7 control gates** between every decision:

GATE	WHAT IT ENFORCES
Confidence Gate	If any agent's confidence drops below a threshold, the decision routes to a human reviewer instead of proceeding automatically
Threshold Gate	Transactions above regulatory limits (NGN 50M+) trigger mandatory enhanced due diligence
Sanctions Block Gate	Confirmed sanctions matches are blocked instantly. No delay. No override without Head of Compliance approval and documented exception
SAR Filing Gate	AI agents draft reports and compile evidence. A human reviews, approves, and files. Always. Non-negotiable.
Escalation Gate	High-risk cases, PEP onboarding, and adverse media matches escalate automatically to senior compliance staff with SLA timers
Identity Failure Gate	Failed identity checks route to a compliance officer. Never silently passed.
Onboarding Gate	New customers are screened before they can transact. Sanctions hits are blocked. PEP matches require C-suite or MLRO approval with documented rationale.

Every gate evaluation is **logged permanently.** When a regulator asks "show me the decision chain for this customer," the answer is one click: the actual chain, with timestamps, confidence levels, agent identifiers, and the name of every person who reviewed it.

Will a Regulator Accept AI in My Compliance Stack?

This is the first question every compliance leader asks. Sentinel is engineered around the answer.

The concern: AI makes mistakes, AI hallucinates, and a regulator will not accept "the algorithm decided." A wrong automated decision is your liability, not the vendor's.

How Sentinel is built to be defensible:

- **AI never files. Humans do.** Agents draft, screen, and analyze. Every reportable action (SAR filing, sanctions override, PEP approval) requires a named human to approve. This is the human-in-the-loop (HITL) control regulators explicitly look for.
- **No black boxes.** Every decision carries its reasoning, the data it used, the confidence score, and the rule or list it matched. Nothing is unexplainable.
- **Uncertainty defers to people.** When an agent is not confident, the confidence gate hands the decision to a human rather than guessing.
- **The model is monitored, not trusted blindly.** The governance dashboard tracks model accuracy, drift, bias, and fairness over time, which is exactly the AI/ML model governance regulators are beginning to require.
- **Every action is tied to a named identity.** The platform runs on authenticated access with least-privilege authority, so each agent and each user acts only within the scope they are permitted, and segregation of duties is enforced rather than assumed. A reviewer cannot approve their own escalation, and the system proves it.
- **Everything is logged and immutable.** The audit trail records who acted, under what authority, and on what evidence, which is the proof that your AI operated under control.

The framing for your regulator: Sentinel does not replace human judgment. It documents it, accelerates it, and makes it provable.

Where Your Data Lives

A compliance buyer will not move without answers on data. Here they are.

- **Deployment is your choice:** cloud-hosted, on-premise, or hybrid. If your regulator or risk appetite requires data to stay in-country or on your own infrastructure, Sentinel deploys on-premise.
- **You own your data and your audit logs.** The immutable decision trail belongs to your institution, exportable for regulator and internal audit.
- **Data residency:** On-premise and hybrid options keep customer and transaction data within your controlled environment, supporting NDPR (Nigeria Data Protection Regulation) and equivalent requirements.
- **Access control:** Authenticated, role-based access maps to your compliance hierarchy (officer, Head of Compliance, MLRO, C-suite). Authority is enforced at every sensitive action, so an under-authorized role cannot approve a decision above its level, and every privileged action is logged against the identity that performed it.
- **Watchlist data** is sourced from official government feeds (OFAC, UN) and refreshed automatically, so your screening is never running against a stale list.

If your team has specific security or data-residency requirements, we map them in the proof-of-concept stage before any live data is touched.

Three-Layer Verification Framework

Sentinel organizes its verification capabilities into three independent layers. Each layer works on its own and the system degrades gracefully when an upstream layer is unavailable.

Layer 3: Watchlist Screening + Continuous Monitoring (LIVE)

- Real sanctions data: OFAC SDN (19,000+ entries) + UN Consolidated (1,000+ entries)
- Auto-refreshes every 6 hours from official government sources
- PEP screening, adverse media indicators
- **Continuous monitoring:** scheduled re-screening of all customers against updated lists
- Delta detection: if a previously clean customer appears on a new list version, an alert fires automatically
- Risk scores are dynamic, not static. They evolve as data changes.

Layer 2: KYC Identity Verification (Integration Ready)

- Provider abstraction built for YouVerify API (Nigeria's leading KYC provider)
- BVN and NIN validation, enhanced PEP screening with Nigerian-specific depth
- Address and business (CAC) verification
- When YouVerify is inactive, the system falls back to rule-based checks. No downtime.

Layer 1: Biometric Verification (Roadmap)

- Fingerprint capture, facial recognition, document OCR
- Provider interface designed for Smile Identity, Veriff, or client-specific hardware
- Deployed per-institution based on their regulatory requirements

Continuous Monitoring: Protection That Never Sleeps

Most AML platforms screen once, at onboarding. Sentinel screens continuously.

How it works:

- Scheduled re-screening runs nightly (configurable: daily, weekly, or on list update)
- Delta detection compares the customer base against newly added watchlist entries
- When a customer's status changes (new sanctions listing, PEP designation, adverse media), an alert is generated automatically
- Risk tiers adjust dynamically: upgrades when new flags appear, de-escalation when flags are cleared and review periods pass
- Monitoring dashboard shows: last run, entities screened, new matches, coverage percentage

Why it matters:

- CBN mandates ongoing customer due diligence, not just onboarding checks
- A customer who was clean in January may be sanctioned by June. Sentinel catches that.
- Your risk picture stays current every single day, not just on the day a customer joined.

Enhanced Transaction Intelligence

Sentinel's Transaction Monitor goes beyond basic threshold checks. It analyzes **8 parameters** across every transaction:

PARAMETER	WHAT IT CATCHES
Regulatory thresholds	Cash and transfer amounts exceeding CBN reporting limits
Velocity burst detection	Sudden 3x+ spike in transaction frequency vs. 90-day baseline
Dormant account reactivation	Account inactive 6+ months suddenly transacting (configurable, CBN standard)
Structuring detection	Multiple transactions just below reporting threshold within 48 hours
Round-tripping	Funds leaving and returning to the same account via intermediaries within 30 days
New account rapid activity	10+ transactions or NGN 5M+ within first 30 days of account opening
Cross-border concentration	30%+ of monthly volume to/from high-risk jurisdictions
Time-of-day anomaly	Transactions outside the customer's established pattern (statistical deviation)

All thresholds are **environment-configurable.** No hardcoded values. Each institution tunes to its own risk appetite.

Executive Escalation Workflow

Not every decision can be automated. Sentinel knows when to escalate and enforces the chain of authority.

How escalation works:

- PEP match at onboarding: escalates to Head of Compliance or C-suite with a 24-hour SLA
- Adverse media match: routes to senior compliance review with evidence summary
- High-value transactions on high-risk accounts: mandatory enhanced due diligence
- Escalations have countdown timers. If the SLA expires without a decision, the system alerts the next level.

Every escalation requires:

- A documented decision (approve or reject)
- Written rationale (mandatory, not optional)
- The approver's identity and timestamp
- The full evidence package that triggered the escalation

This is what regulators mean by "demonstrable human oversight."

CBN Compliance Coverage

Sentinel addresses **90% of CBN requirements today**, rising to **95% with Phases 1 through 3 of the roadmap.**

CBN SECTION	COVERAGE
Risk Assessment and Customer Profiling	100%
Sanctions and PEP Screening	100%
Transaction Monitoring (all channels)	100%
Investigation and Case Management	100%
Regulatory Reporting (STRs, CTRs, summaries)	100%
Audit Trail and Governance Documentation	100%
AI/ML Model Governance (accuracy, drift, bias, fairness tracking)	100%
Customer Identification / KYC	75% (full with YouVerify)
Know Your Business / KYB	50% (full with YouVerify + CAC)

Remaining 5%: Biometric verification hardware (institution-specific) and full document management system. These are deployment-time integrations, not software gaps.

The Dashboard: Full Visibility in One Place

Sentinel's interface gives compliance teams everything in one place:

1. **Dashboard:** KPIs at a glance. Transactions monitored, flagged, open alerts, average agent confidence, regulatory alignment indicators (FATF, CBN, NFIU, HITL status)
2. **Customer Onboarding:** New customer screening queue, status badges (Screening, Clear, Pending Approval, Blocked), escalation panel with approve/reject
3. **Transactions:** Full transaction list with real-time screening. Run any transaction through the 7-agent pipeline on demand.
4. **Alerts:** Generated alerts with risk scores, affected customers, triggered rules
5. **Watchlist Screening:** Sanctions, PEP, and adverse media matches. Categorized with color-coded badges (red for sanctions, orange for PEP, yellow for adverse media)
6. **SARs:** Suspicious Activity Reports drafted by AI, awaiting human approval. Full evidence packages attached. Human approval required banner.
7. **Cases:** Investigation case management with deadlines, assignments, escalation tracking
8. **Governance:** Immutable audit trail. Every agent decision logged. Model validation dashboard tracking accuracy, drift, bias, and fairness over time.

How It Fits Into Your Existing Systems

Sentinel does not replace your core banking system, payment gateway, or existing tools. It connects to them.

Integration:

- Your transaction system sends data to Sentinel through a REST API
- Sentinel processes it through the full agent pipeline and returns a risk decision
- Flagged transactions, alerts, and cases appear on the dashboard
- SARs are drafted automatically and wait for human approval before filing

Deployment options:

- Cloud-hosted (fastest, lowest upfront cost)
- On-premise (strict data residency requirements)
- Hybrid (compute in cloud, data on-premise)

Tech stack: FastAPI + Next.js + LangChain + SQLite/PostgreSQL. Modern, maintainable, and auditable.

Investment

Enterprise AML platforms cost **$500K to $2M+** in licensing alone, plus multi-year implementations. Sentinel is built to deliver the same core capabilities at a fraction of that, with a pricing model designed for institutions that need to comply now.

How pricing works:

- **Annual platform subscription** scaled to your institution size (transaction volume and customer base), so a microfinance bank is not priced like a tier-1 commercial bank
- **One-time implementation and integration fee** covering proof of concept, integration to your core systems, and team training
- **Optional add-ons** billed as used: KYC verification provider (YouVerify), biometric verification, on-premise deployment support

What is included in every tier:

- All 7 agents and the full governance engine
- Continuous monitoring and automatic watchlist refresh
- The full 8-tab dashboard
- The complete audit trail and model governance dashboard

We size a specific quote during the proof of concept, once we see your transaction volume and deployment needs. The proof of concept itself is structured to prove value before you commit to the platform.

Getting Started: A Risk-Free Path to Production

Stage 1: Proof of Concept (2 to 4 weeks) Run Sentinel against your historical transactions. Compare what it catches against what your team found manually. See the governance trail in action. This is where your own numbers (false-positive reduction, time saved, missed risks surfaced) get measured.

Stage 2: Shadow Mode (4 to 8 weeks) Run Sentinel alongside your current compliance process. Your team keeps working. Sentinel runs in parallel. You compare results and tune thresholds. Zero disruption to live operations.

Stage 3: Go Live (4 to 6 weeks) Connect to live transactions. Enable real-time screening. Integrate identity verification providers. Train your compliance team on the dashboard.

Total: 10 to 18 weeks from kickoff to production.

Your June 2026 compliance roadmap submission can reference a system already in testing.

Why Sentinel

WHAT MATTERS	SENTINEL
Built for Nigeria	CBN thresholds, NGN amounts, NFIU reporting format, Nigerian domestic watchlists. Not a global platform adapted after the fact.
Globally transferable	The governance architecture (confidence gates, HITL enforcement, audit trails, model validation) maps to OSFI, FCA, FinCEN, and FATF requirements.
Affordable	Enterprise AML platforms cost $500K to $2M+. Sentinel delivers the same capabilities at a fraction of the cost.
Fast to deploy	Weeks, not years. Shadow mode means zero disruption to current operations.
Full lifecycle	From customer onboarding to continuous monitoring. Not just transaction screening.
Transparent	Every decision logged and explainable. No black boxes. When the regulator asks, you have the answer.
Human oversight built in	AI handles the volume. People make the final calls. That is not just good practice. It is what the CBN requires.

Let's Talk

Sentinel is live today at **sentinel.veristack.ca**. You can see it working right now.

Next step: A 30-minute walkthrough where we screen transactions in real time and show you the full compliance chain from customer onboarding to alert to SAR to audit trail. Bring a sample of your own transaction patterns and we will show you what Sentinel surfaces.

Wale Aderonmu Founder, VeriStack Inc. wale@veristack.ca veristack.ca

> Innovate Boldly, Scale Securely.

Appendix: Glossary

- **AML:** Anti-Money Laundering
- **CBN:** Central Bank of Nigeria (the regulator issuing the directive)
- **NFIU:** Nigerian Financial Intelligence Unit (receives SAR/STR filings)
- **SAR / STR:** Suspicious Activity Report / Suspicious Transaction Report
- **CTR:** Currency Transaction Report
- **MLRO:** Money Laundering Reporting Officer (the accountable compliance role)
- **PEP:** Politically Exposed Person (higher-risk customer requiring enhanced scrutiny)
- **KYC / KYB:** Know Your Customer / Know Your Business
- **BVN / NIN:** Bank Verification Number / National Identification Number (Nigerian identity records)
- **CAC:** Corporate Affairs Commission (Nigerian business registry)
- **HITL:** Human-in-the-Loop (a human approves before a consequential action)
- **PSP / MMO:** Payment Service Provider / Mobile Money Operator
- **EDD:** Enhanced Due Diligence
- **OFAC / UN lists:** Sanctions lists used for watchlist screening
- **NDPR:** Nigeria Data Protection Regulation
