

ANTI-CALL MASKING PLATFORM

System Overview Training

Duration: ~15 minutes

Audience: All Staff

Version: 2.0 | January 2026

AGENDA

1. What is Call Masking Fraud?
2. How Our System Works
3. Key Components
4. Performance & Capabilities
5. NCC Compliance
6. Your Role in the System

WHAT IS CALL MASKING FRAUD?

Understanding the threat we protect against

CALL MASKING EXPLAINED

Definition: Call masking (CLI spoofing) is when fraudsters use multiple fake caller IDs to reach the same victim.

HOW ATTACKERS OPERATE:

- Generate dozens of fake phone numbers
- Call the same victim from different "identities"
- Evade traditional fraud detection
- Execute scams with apparent legitimacy

THE ATTACK PATTERN

Attacker System

Generates
Fake IDs

+234-801-1111
+234-802-2222
+234-803-3333
+234-804-4444
+234-805-5555

Victim

+234-XXX

5+ different numbers → Same destination → Within seconds

IMPACT ON NIGERIA

₦15B+

Annual Fraud Losses

₦5B+

Customer Churn

₦2B+

Regulatory Fines

Beyond financial losses, call masking damages consumer trust in telecommunications.

HOW OUR SYSTEM WORKS

Real-time fraud detection in milliseconds

DETECTION LOGIC

WE MONITOR:

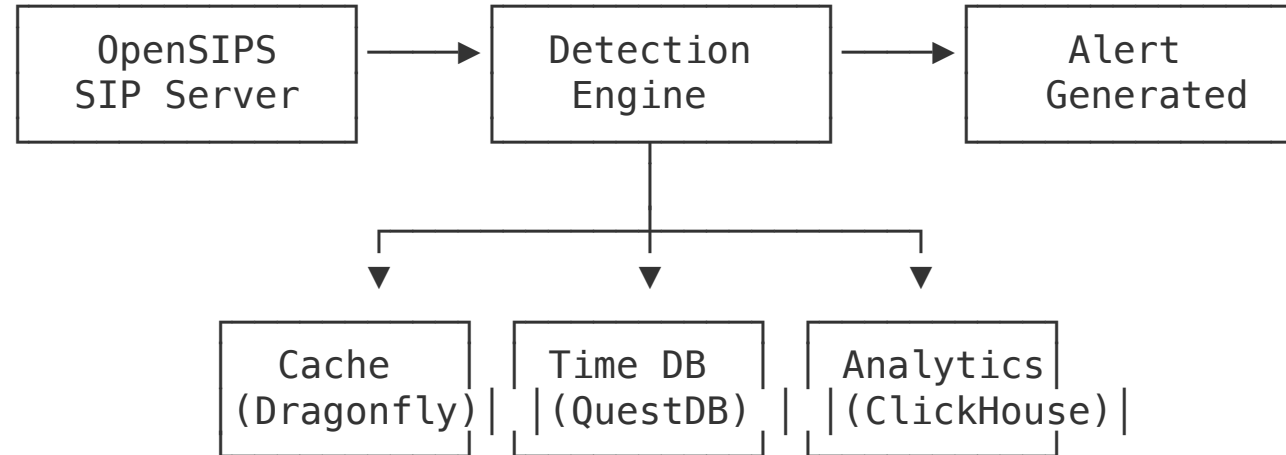
- **A-Numbers:** Callers
(source)
- **B-Numbers:** Destinations
(target)
- **Time Windows:** Calls
within seconds

WE DETECT:

- 5+ different callers
- Same destination
- Within 5 seconds

Result: Fraudulent calls are detected and can be automatically disconnected

PROCESSING FLOW



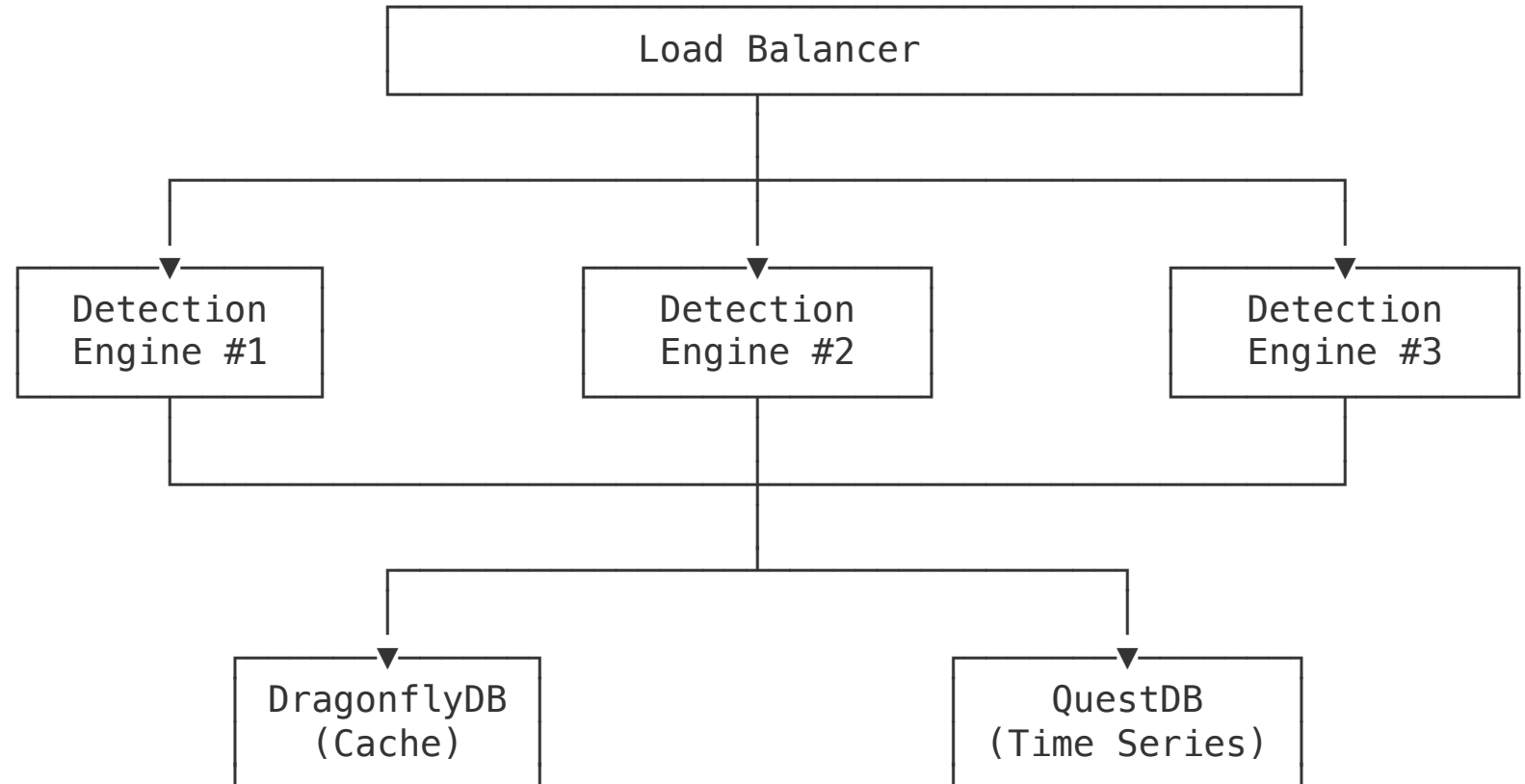
RESPONSE ACTIONS

Detection	Action	Time
Pattern Identified	Alert Generated	< 1ms
Alert Created	SOC Notified	Immediate
Auto-disconnect Enabled	Calls Terminated	< 5ms
NCC Reporting	Daily Upload	06:00 WAT

KEY COMPONENTS

The building blocks of our platform

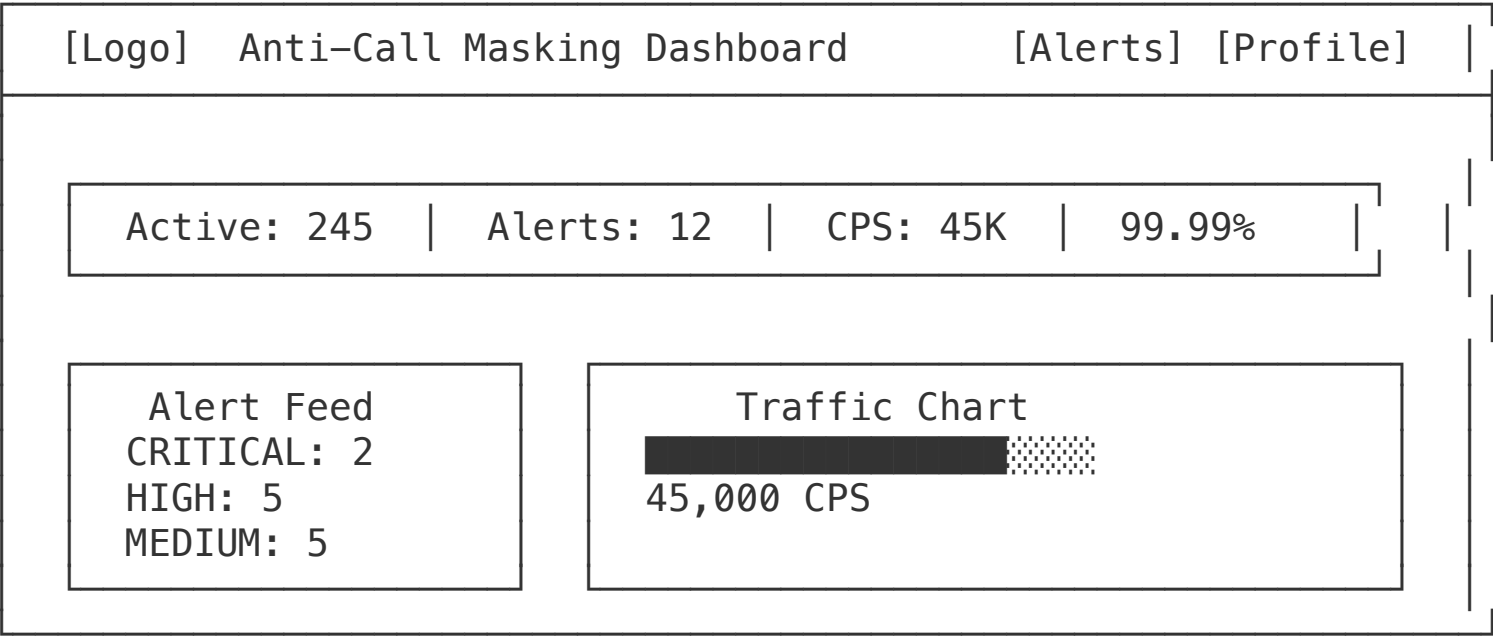
SYSTEM ARCHITECTURE



COMPONENT ROLES

Component	Purpose
Detection Engine	Real-time fraud detection (Rust)
DragonflyDB	In-memory sliding window cache
QuestDB	Time-series event storage
YugabyteDB	Configuration and alert storage
ClickHouse	Long-term analytics
Management API	Dashboard and integrations

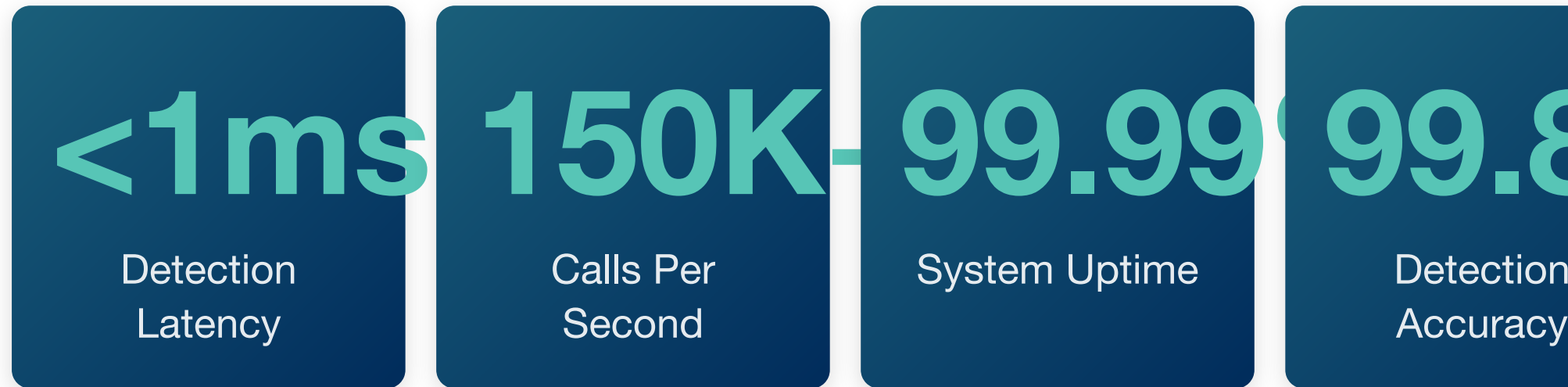
DASHBOARD INTERFACE



PERFORMANCE & CAPABILITIES

Industry-leading speed and scale

KEY PERFORMANCE METRICS



WHY WE'RE FAST

- **Rust Engine:** Memory-safe, zero-cost abstractions
- **io_uring:** Kernel-bypass I/O for minimal latency
- **In-Memory Cache:** DragonflyDB for microsecond lookups
- **Lock-Free Design:** No contention bottlenecks
- **Horizontal Scaling:** Add nodes as traffic grows

COMPARISON TO ALTERNATIVES

Feature	ACM Platform	Industry Standard
Detection Latency	< 1ms	100ms+
Throughput	150K+ CPS	10K CPS
Detection Mode	Real-time	Post-processing
NCC Integration	Native	Manual

NCC COMPLIANCE

Meeting regulatory requirements

REGULATORY FRAMEWORK

The **Nigerian Communications Commission (NCC)** requires all telecom operators to implement fraud detection and report incidents.

OUR COMPLIANCE FEATURES:

- Automated daily report generation
- SFTP upload to NCC by 06:00 WAT
- ATRS (Automated Trouble Reporting System) integration
- 5-year audit log retention

DAILY NCC REPORT

Field	Description
Incident ID	Unique alert identifier
Detection Time	When attack was detected
B-Number	Targeted destination
A-Number Count	Number of spoofed callers
Action Taken	Response (blocked/alerted)
Resolution	Final disposition

COMPLIANCE DASHBOARD

Current Status: All NCC requirements met

- ✓ Daily reports submitted on time
- ✓ ATRS integration active
- ✓ Audit logs retained (5 years)
- ✓ Data residency compliant
- ✓ Monthly summaries generated

YOUR ROLE IN THE SYSTEM

How different teams interact with ACM

SOC ANALYSTS

RESPONSIBILITIES:

- Monitor real-time alerts
- Investigate suspicious patterns
- Take action on confirmed fraud
- Document incidents

KEY TOOLS:

- Alert Dashboard
- Investigation View
- Disconnect Controls
- Whitelist Management

NETWORK ADMINISTRATORS

RESPONSIBILITIES:

- Monitor system health
- Manage capacity
- Deploy updates
- Troubleshoot issues

KEY TOOLS:

- Grafana Dashboards
- Prometheus Alerts
- Docker/Kubernetes
- Log Analysis

COMPLIANCE OFFICERS

RESPONSIBILITIES:

- Verify NCC compliance
- Review reports
- Support audits
- Track regulations

KEY TOOLS:

- NCC Reports Section
- Audit Log Viewer
- Compliance Dashboard
- Export Functions

EXECUTIVES

WHAT YOU SEE:

- Fraud reduction metrics
- System ROI
- Compliance status
- Trend analysis

KEY DASHBOARDS:

- Executive Summary
- Monthly Reports
- KPI Tracking
- Benchmark Data

SUMMARY

- **Call masking** is a serious fraud threatening Nigerian telecom
- Our platform detects attacks in **under 1 millisecond**
- We process **150,000+ calls per second**
- **NCC compliance** is fully automated
- Every team has a role in protecting our network

QUESTIONS?

Additional Training Available:

- Admin Training (30 min)
- SOC Analyst Training (45 min)
- Developer Training (45 min)

Documentation: </docs/>

Support: support@yourcompany.com

THANK YOU

Anti-Call Masking Platform

Protecting Nigerian Telecommunications
www.yourcompany.com