PRE-DEAL INTELLIGENCE REPORT · CBN AML/CFT COMPLIANCE ASSESSMENT

AML/CFT COMPLIANCE GAP ANALYSIS

Central Bank of Nigeria — Circular BSD/DIR/PUB/LAB/019/002

PREPARED FOR

NovaPay Financial Technologies Ltd.

Lagos, Nigeria · Financial Technology — Payment Processing · Series A Funded
CBN Payment Service Provider Licenced · NIBSS Connected · 47 Employees
■2.4 Billion Monthly Transaction Volume · 180,000+ Transactions · 340 Agent Locations

OVERALL COMPLIANCE POSTURE SCORE

23 / 100

0 — NON-COMPLIANT · 50 — PARTIAL · 100 — FULLY COMPLIANT

5	3	4	2
CRITICAL	HIGH	MEDIUM	LOW

CRITICAL — IMMEDIATE REMEDIATION REQUIRED PRIOR TO CBN EXAMINATION

CRITICAL FINDINGS REQUIRING IMMEDIATE REGULATORY ACTION

F-001	No real-time AML transaction monitoring system deployed — CBN Requirement 1 completely unmet
F-002	Automated STR/CTR generation absent — manual process cannot satisfy NFIU submission timelines
F-003	Agent network (■744M monthly, 31% of total volume) operating entirely outside monitoring scope
F-004	No ML-based behavioural analytics or pattern detection capability — CBN Requirement 2 unmet
F-005	NIN integration absent — 28,140 existing customer accounts with incomplete KYC verification

THIS REPORT CONTAINS

- → Complete gap analysis across all five CBN AML/CFT requirements
- → Fourteen findings — each with evidence basis, risk rating, and remediation instruction
- → Thirty-day prioritised remediation roadmap with assigned owners and defined outputs
- → Risk matrix ranking all findings by regulatory exposure and business impact
- → Recommended StackWeaver engagement and investment to achieve full compliance

WHAT YOU ARE LOOKING AT

This document is the Executive Intelligence Deliverable produced at the commencement of every StackWeaver compliance engagement. It is a diagnostic assessment — not a regulatory filing, not an audit opinion, and not a substitute for full workpaper-grade evidence. Read the comparison below before proceeding.

WHAT THIS DOCUMENT IS	WHAT THIS DOCUMENT IS NOT	WHAT YOU RECEIVE IN THE PAID ENGAGEMENT
A Board-ready gap analysis produced from publicly available information and submitted company data. — Overall compliance posture score — 14 findings across all CBN requirements — Risk matrix ranked by regulatory exposure — 30-day owner-assigned remediation roadmap — Directionally accurate and independently verified by a senior compliance engineer	A regulatory filing. An audit opinion. A document that can be submitted to the CBN as evidence of compliance. This report does not contain re-performance testing, system access validation, transaction log sampling, API call evidence, or the workpaper package that regulators require. The gaps identified are real. The evidence that satisfies the regulator is produced only in the paid engagement.	This executive report PLUS: — Full workpaper package with re-performance testing — System screenshots and API call logs — Transaction sample testing (25–40% of key items) — CBN and NFIU-ready evidence binder — 200–400 automated QA tests generating compliance evidence simultaneously — StackWeaver Commitment Guarantee on all scoped gaps — Posture score 85+ at engagement completion

INDEPENDENCE AND SCOPE STATEMENT This assessment was conducted by StackWeaver on the basis of publicly available information, submitted company data, and open-source intelligence gathered through StackWeaver's Posture Intelligence Engine. StackWeaver is not a licensed auditor and does not attest to, certify, or provide audit opinions on compliance status. This report constitutes a gap analysis and readiness assessment only. All findings were reviewed and verified by Emmanuel O., Senior Compliance Engineer — 12 years in CBN-regulated financial institutions, AML/CFT specialist, ex-KPMG Advisory, Certified Anti-Money Laundering Specialist (CAMS) — prior to delivery. StackWeaver's analysis does not replace independent legal counsel or a licensed auditor's opinion. NovaPay Financial Technologies Ltd. should engage qualified legal counsel for advice specific to its obligations under CBN supervision.

REDACTED SAMPLE · NovaPay Financial Technologies Ltd. — Series A PSP, Lagos, Nigeria · Engagement SW-2026-CBN-001 · This is a redacted sample of the executive deliverable. Full workpaper-grade evidence, re-performance testing, and system-access validation are delivered exclusively in the paid engagement. StackWeaver's Commitment Guarantee applies only to gaps closed under full paid engagement scope.

ENGAGEMENT OVERVIEW

CLIENT		ENGAGEMENT REF	SW-2026-CBN-001
FRAMEWORK	CBN Circular BSD/DIR/PUB/LAB/019/002	DATE OF ISSUE	March 2026
INDUSTRY	Financial Technology — Payment Processing (PSP)	DOCUMENT STATUS	**DRAFT — PENDING CLIENT REVIEW**
JURISDICTION	Lagos, Nigeria — CBN Regulated Institution	CLASSIFICATION	**STRICTLY CONFIDENTIAL**
TRANSACTION VOLUME	■2.4 Billion monthly — 180,000+ transactions	OVERALL POSTURE SCORE	**23 / 100 — CRITICAL**
ORGANISATION SIZE	47 employees across Engineering, Compliance and Operations	PREPARED BY	StackWeaver — AI-Powered Analysis, Senior Compliance Expert Review

TABLE OF CONTENTS

01 EXECUTIVE SUMMARY AND BOARD-LEVEL ASSESSMENT

Prepared for the Board of Directors and Executive Leadership Team — NovaPay Financial Technologies Ltd.

StackWeaver conducted a comprehensive AML/CFT compliance gap analysis of NovaPay Financial Technologies Ltd. ('NovaPay') against the requirements of the Central Bank of Nigeria's Circular BSD/DIR/PUB/LAB/019/002. The assessment evaluates NovaPay's technology infrastructure, compliance processes, and operational controls against each of the five mandatory requirements prescribed in the circular.

The findings are unambiguous. NovaPay is currently processing ■2.4 billion monthly across 180,000 transactions without the monitoring infrastructure the CBN mandates. Of the five core requirements, none are fully met. The overall compliance posture score of 23 out of 100 reflects an institution that has implemented foundational compliance processes but has not yet constructed the technology infrastructure required to satisfy the CBN's specific mandates for real-time monitoring, automated reporting, and unified customer screening.

CBN REQUIREMENT	STATUS	SCORE	ASSESSMENT SUMMARY
Req 1 — Real-Time AML Transaction Monitoring	NOT MET	0 / 20	No monitoring system deployed. Manual T+1 review only. Direct regulatory violation.
Req 2 — Advanced Analytics and Pattern Detection	NOT MET	3 / 20	Static threshold rules only. No machine learning or behavioural analytics.
Req 3 — Unified AML Screening Platform	PARTIAL	8 / 20	Point-in-time screening only. Not unified across all product channels.
Req 4 — BVN/NIN Integration and Verification	PARTIAL	7 / 20	BVN integrated via NIBSS. NIN absent. 28,140 accounts with incomplete KYC.
Req 5 — Automated STR/CTR Reporting	NOT MET	5 / 20	Manual STR process. CTR automation absent. NFIU timeline compliance at risk.
OVERALL POSTURE SCORE	CRITICAL	23 / 100	**Five critical gaps identified. Immediate remediation required.**

Board-Level Risk Assessment

The institution faces two categories of risk arising from the current compliance posture. The first is regulatory: CBN examination of NovaPay's AML infrastructure at current maturity would constitute a direct finding of non-compliance against Requirements 1, 2, and 5, with material risk of sanction, operational restriction, or licence review. The second is operational: NovaPay is processing substantial transaction volumes across multiple channels without the detection infrastructure required to identify financial crime in real time. The exposure is not theoretical — it is active.

Of particular concern is the agent network. Three hundred and forty agent locations processing an estimated ■744 million monthly — 31 percent of NovaPay's total transaction volume — are operating entirely outside the compliance monitoring scope. Cash-in and cash-out transactions through agents represent the highest-risk channel in NovaPay's operating model. The absence of monitoring on this channel is the single most significant financial crime exposure identified in this assessment.

02 COMPANY AND RISK PROFILE

NovaPay Financial Technologies Ltd. is a Lagos-based payment processing platform serving retail consumers and small-to-medium enterprises across Nigeria. The company holds a CBN Payment Service Provider licence and processes transactions across mobile money, card payments, USSD, and inter-bank transfers through both a direct digital platform and an agent network.

ATTRIBUTE	DETAIL	AML/CFT RISK IMPLICATION
Monthly transaction volume	■2.4 billion — 180,000+ transactions	HIGH — Volume materially exceeds the capacity of manual monitoring to achieve meaningful coverage.
Customer base	42,000 active retail users; 1,200 SME accounts	HIGH — Large retail base with limited transaction transparency increases layering and smurfing risk.
Agent network	340 locations; est. ■744M/month (31% of volume)	CRITICAL — Cash-in/cash-out channel is NovaPay's highest-risk channel and is currently unmonitored.
Geographic reach	14 states — Lagos-concentrated; northern state exposure	MEDIUM — Northern state activity requires enhanced due diligence protocols.
Regulatory status	CBN PSP Licence; NIBSS connected	CRITICAL — Direct CBN supervisory relationship means examination risk is immediate and ongoing.
Current AML tooling	Manual review; basic threshold alerts; Excel-based flagging	CRITICAL — Manual processes cannot satisfy the CBN's real-time monitoring mandate at current volumes.

03 CBN AML/CFT FRAMEWORK — MANDATORY REQUIREMENTS

The CBN Circular BSD/DIR/PUB/LAB/019/002 prescribes five specific technology capabilities for all regulated financial institutions. These represent mandatory compliance requirements. Non-compliance exposes institutions to regulatory sanction, operational restriction, and licence consequences under CBN examination.

REQ	REQUIREMENT	CBN MANDATE	NOVAPAY STATUS
01	Real-Time AML Transaction Monitoring	Automated, real-time monitoring of all transactions against defined AML typology rules and risk parameters, across all product channels.	NOT MET
02	Advanced Analytics and Pattern Detection	Machine learning-driven behavioural analytics for detecting unusual patterns, velocity anomalies, and network-level financial crime risk across the customer base.	NOT MET
03	Unified AML Screening Platform	A single platform screening all customers and transactions against applicable sanctions lists, PEP databases, adverse media sources, UN and OFAC designations.	PARTIAL
04	BVN/NIN Integration and Verification	Real-time BVN and NIN verification at customer onboarding, with ongoing reverification of the existing customer base.	PARTIAL
05	Automated STR/CTR Reporting	Automated generation and timely submission of Suspicious Transaction Reports and Cash Transaction Reports to the NFIU via goAML API, within mandated timelines.	NOT MET

04 CRITICAL GAP ANALYSIS

Five critical findings presented in full. Each finding is substantiated by specific evidence and accompanied by a defined remediation action. Nine additional High, Medium and Low findings are summarised in Section 06.

FINDING-001	CRITICAL	Remediation effort: Eight to twelve weeks	Priority sequence: First — Immediate
No Real-Time AML Transaction Monitoring System Deployed			
CBN REQUIREMENT	CBN Requirement 1 — Automated real-time monitoring of all transactions against AML typology rules.		
CURRENT STATE	NovaPay relies on manual transaction review conducted by two compliance staff members. Reviews are performed on a T+1 basis — the day following transaction execution. A basic threshold alert system flags items for manual review. No automated monitoring engine is deployed across any transaction channel.		
GAP IDENTIFIED	Real-time monitoring is explicitly mandated by the circular. T+1 manual review does not constitute real-time monitoring under any reasonable interpretation of the requirement. At 180,000 or more monthly transactions, two compliance staff cannot achieve the coverage required — the arithmetic makes comprehensive manual review impossible.		
EVIDENCE BASIS	Technical architecture review confirms no AML monitoring platform is deployed. Current tooling consists of an Excel-based flagging system with a manual review queue. No Napier, Actimize, Temenos Financial Crime Mitigation or equivalent platform is in place.		
RISK IMPACT	Direct CBN examination finding — near-certain regulatory sanction upon discovery. Financial crime flowing through the platform at scale, undetected. Material regulatory, operational, and reputational exposure.		
REMEDIATION ACTION	Procure and deploy an AML transaction monitoring platform with real-time rule execution. Configure typology rules specific to NovaPay's transaction profiles across all channels. Establish alert triage workflows with defined SLAs. Priority vendors for evaluation: Napier AI, Temenos Financial Crime Mitigation, NetReveal.		

FINDING-002	CRITICAL	Remediation effort: Six to eight weeks	Priority sequence: Second — Immediate
Automated STR/CTR Generation and Submission Absent			
CBN REQUIREMENT	CBN Requirement 5 — Automated generation and timely submission of STRs and CTRs via goAML.		

CURRENT STATE	Suspicious Transaction Reports are generated manually by the compliance team following threshold alert review. Cash Transaction Reports are produced on a monthly batch basis. Neither process is automated. The compliance team manually prepares reports in the NFIU prescribed format and submits via the goAML web portal. No goAML API integration exists.
GAP IDENTIFIED	The CBN circular requires automated report generation. Manual preparation introduces processing delays, creates risk of missed reporting windows, and produces documentation inconsistencies. The NFIU's 24-hour STR submission requirement cannot be reliably met with manual processes, particularly when the compliance team is concurrently managing all other compliance obligations.
EVIDENCE BASIS	Compliance workflow review confirms manual STR preparation. No goAML API integration identified. CTR batching occurs monthly, not within the required timeframe for transactions exceeding the ■5,000,000 threshold.
RISK IMPACT	Regulatory sanctions for late or missed STR and CTR submissions. NFIU examination findings. Reputational risk arising from association with unreported suspicious activity.
REMEDIATION ACTION	Integrate the goAML API to enable automated STR and CTR generation and submission. Configure the ■5,000,000 threshold trigger for automated CTR generation. Build the complete STR workflow from monitoring system alert through to NFIU submission, with a full audit trail at every stage.

FINDING-003	CRITICAL	Remediation effort: Four to six weeks following platform deployment	Priority sequence: Third — Critical
Agent Network Processing ■744 Million Monthly Outside Monitoring Scope			
CBN REQUIREMENT	CBN Requirement 1 — All transaction channels must be covered by real-time monitoring.		
CURRENT STATE	NovaPay's 340-location agent network is not integrated with the compliance monitoring infrastructure. Agent network transactions — estimated at ■744 million monthly, representing 31 percent of total transaction volume — are reviewed manually on a weekly basis via a standalone agent portal with no connection to compliance systems.		
GAP IDENTIFIED	The agent network represents NovaPay's highest-risk transaction channel. Cash-in and cash-out transactions conducted through agents are primary vehicles for structuring, smurfing, and trade-based money laundering typologies. Having 31 percent of total transaction volume operating outside any monitoring scope is an indefensible gap under the circular's all-channel coverage mandate.		
EVIDENCE BASIS	Agent transaction data confirmed as residing in a separate system with no API connection to compliance tooling. The agent portal operates independently of the core transaction stack. Weekly manual review represents a monitoring lag wholly incompatible with the CBN's real-time requirement.		
RISK IMPACT	Direct regulatory non-compliance with Requirement 1's all-channel coverage mandate. NovaPay is operationally blind to financial crime on its highest-risk and highest-concentration channel.		
REMEDIATION ACTION	Integrate the agent network transaction feed into the AML monitoring platform via API immediately upon platform deployment. Configure agent-specific typology rules covering structuring detection, cash velocity limits, and geographic anomaly identification. Implement real-time monitoring across all agent locations from the first day of platform operation.		

FINDING-004	CRITICAL	Remediation effort: Twelve to sixteen weeks	Priority sequence: Fourth — High
No Machine Learning Analytics or Behavioural Pattern Detection Capability			
CBN REQUIREMENT	CBN Requirement 2 — Advanced analytics including machine learning for pattern detection.		

CURRENT STATE	NovaPay's compliance infrastructure relies on static, threshold-based rules configured approximately 18 months ago. These rules have not been reviewed or updated since initial deployment. No machine learning models are in operation for behavioural profiling, peer group analysis, network analytics, or anomaly detection. The data science function, comprising two engineers, is focused exclusively on product analytics.
GAP IDENTIFIED	Static rules detect known typologies. Machine learning analytics detect evolving ones. The CBN circular explicitly requires advanced analytics capability — static threshold rules do not satisfy this requirement regardless of how carefully they are calibrated. Financial crime methodologies evolve continuously; static rules create a detection ceiling that sophisticated actors will exploit.
EVIDENCE BASIS	Technical stack review confirms no ML-based AML tooling in operation. Rules engine is a basic threshold configuration. No entity resolution, network analytics, or behavioural baseline capability identified.
RISK IMPACT	Regulatory non-compliance with Requirement 2. Sophisticated layering and network-based financial crime schemes will not be detected by threshold rules alone. Criminal exposure compounds as transaction volumes grow.
REMEDIATION ACTION	Procure an AML monitoring platform with embedded machine learning analytics, or integrate a specialist ML layer with the primary monitoring system. Configure entity resolution and network analytics for connected account identification. Establish a model governance framework and ongoing performance monitoring process.

FINDING-005	CRITICAL	Remediation effort: Three to four weeks for integration; eight weeks for retroactive campaign	Priority sequence: Fifth — Immediate
NIN Integration Absent — 28,140 Customer Accounts with Incomplete KYC			
CBN REQUIREMENT	CBN Requirement 4 — Real-time BVN and NIN verification at onboarding and on an ongoing basis.		
CURRENT STATE	BVN verification is integrated at the point of customer onboarding via NIBSS. NIN verification is not integrated. Approximately 67 percent of NovaPay's existing customer base — estimated at 28,140 accounts — were onboarded prior to the NIN mandate and have not been retroactively verified. The NIN field is absent from the current customer registration flow.		
GAP IDENTIFIED	NIN is a mandatory verification requirement alongside BVN. Without NIN integration, NovaPay cannot confirm the identity of customers whose BVN credentials may be fraudulent or misappropriated. The 28,140 accounts without NIN on file represent a known and quantifiable population of customers with materially incomplete KYC.		
EVIDENCE BASIS	Onboarding workflow review confirms NIN field is absent from customer registration. NIBSS BVN API is integrated. NIMC NIN verification API is not integrated. Customer database export confirms 28,140 accounts without NIN on file.		
RISK IMPACT	Direct CBN non-compliance with Requirement 4. 28,140 customers with incomplete KYC, each representing an unquantified financial crime exposure in the customer base.		
REMEDIATION ACTION	Integrate NIN verification via the NIMC API or an approved third-party NIN service provider. Implement mandatory NIN capture at point of onboarding for all new customers. Launch a structured retroactive NIN collection programme for the 28,140 existing accounts, with a defined deadline after which non-compliant accounts are subject to transaction restriction.		

05 HIGH AND MEDIUM FINDINGS — SUMMARY

Nine additional findings across requirements. Full documentation available in the complete engagement report.

ID	FINDING	SEVERITY	REQUIREMENT	REMEDIATION SUMMARY
F-006	Customer risk scoring absent — no dynamic tiering of customer risk profiles	HIGH	Req 2	Implement risk-based customer scoring model with Low, Medium, High and PEP tiers.
F-007	PEP screening conducted on a point-in-time basis only — not continuous	HIGH	Req 3	Migrate to continuous PEP and sanctions screening via an integrated screening provider.
F-008	Adverse media screening absent across the entire customer base	HIGH	Req 3	Add adverse media screening layer to the unified screening platform.
F-009	Enhanced Due Diligence process not documented for high-risk customers	MEDIUM	Req 1, 2	Document and implement an EDD protocol for High and PEP tier customers.
F-010	AML typology rules not reviewed or updated in 18 months	MEDIUM	Req 1	Establish a quarterly typology review process with documented senior sign-off.
F-011	USSD channel transactions not subject to AML monitoring	MEDIUM	Req 1	Extend monitoring platform integration to the USSD transaction feed.
F-012	No pre-submission STR quality review process in place	MEDIUM	Req 5	Implement a pre-submission STR quality review checklist with senior compliance sign-off.
F-013	AML training records incomplete — 23 of 47 staff without documented training	MEDIUM	General	Conduct mandatory AML training for all 47 staff with documented completion records.
F-014	No documented AML governance framework or MLRO terms of reference	LOW	General	Document the MLRO role, AML governance structure, and escalation protocols.

06 RISK MATRIX — ALL FOURTEEN FINDINGS RANKED

Rankings reflect regulatory risk (probability and severity of CBN examination finding) and business impact (financial, operational and reputational consequence).

ID	FINDING	REGULATORY RISK	BUSINESS IMPACT	RISK SCORE	SEQUENCE
F-001	No real-time transaction monitoring	**CRITICAL**	**CRITICAL**	**95 / 100**	1
F-003	Agent network unmonitored (31% of volume)	**CRITICAL**	**CRITICAL**	**92 / 100**	2
F-002	Automated STR/CTR reporting absent	**CRITICAL**	**CRITICAL**	**91 / 100**	3
F-005	NIN absent — 28,140 KYC gap	**CRITICAL**	**HIGH**	**87 / 100**	4
F-004	No ML analytics or pattern detection	**HIGH**	**HIGH**	**76 / 100**	5
F-006–F-008	Three High findings — screening gaps	**HIGH**	MIXED	55–68	6–8
F-009–F-013	Five Medium findings — process gaps	**MEDIUM**	MIXED	28–45	9–13
F-014	One Low finding — governance documentation	**LOW**	LOW	18 / 100	14

07 THIRTY-DAY REMEDIATION ROADMAP

Sequenced to achieve the maximum reduction in regulatory exposure within thirty days. Owners reflect NovaPay's current organisational structure.

PERIOD	ACTION	RESPONSIBLE OWNER	FINDING	DELIVERABLE
Days 1–3	Issue request for proposal to AML monitoring vendors. Evaluate Napier AI, Temenos Financial Crime Mitigation and NetReveal. Select vendor and execute contract.	CTO + CISO	**F-001**	Vendor selected and contracted.
Days 1–5	Integrate NIMC NIN verification API at customer onboarding. Initiate retroactive NIN collection programme for 28,140 existing accounts.	Engineering	**F-005**	NIN live at onboarding. Collection campaign active.
Days 3–10	Integrate goAML API for automated STR and CTR generation. Configure ■5,000,000 CTR threshold trigger. Build submission workflow with audit trail.	Compliance and Engineering	**F-002**	Automated reporting pipeline operational.
Days 7–14	Begin AML monitoring platform deployment. Connect core transaction data feed. Deploy initial typology rule set and establish alert triage process.	CTO and Vendor	**F-001**	Platform ingesting live transaction data.

PERIOD	ACTION	RESPONSIBLE OWNER	FINDING	DELIVERABLE
Days 14–21	Integrate agent network transaction feed into monitoring platform. Configure agent-specific typology rules, cash velocity thresholds, and geographic anomaly detection.	Engineering	**F-003**	Agent network under real-time monitoring.
Days 21–30	Tune monitoring rules against NovaPay's actual transaction profile. Validate alert accuracy and false positive rate. Deliver mandatory AML training to all staff.	Compliance	**F-001, F-013**	Monitoring operational. Team trained and certified.
Day 30+	Phase 2: Machine learning analytics integration, unified screening platform deployment, resolution of remaining High and Medium findings.	StackWeaver and NovaPay	F-004–F-014	Full CBN compliance achieved.

08 RECOMMENDED NEXT STEPS

Sequenced remediation actions for NovaPay's executive and compliance leadership team.

The findings in this report represent an accurate and current assessment of NovaPay's AML/CFT compliance posture against the requirements of CBN Circular BSD/DIR/PUB/LAB/019/002. Five critical gaps require immediate action. The following steps are recommended in order of regulatory priority.

PRIORITY	ACTION REQUIRED	RESPONSIBLE	DEADLINE
1 — CRITICAL	Procure and contract an AML transaction monitoring platform. Recommended evaluation: Napier AI, Temenos Financial Crime Mitigation, NetReveal.	CTO and Board	**Days 1–3**
2 — CRITICAL	Integrate NIMC NIN verification API. Launch retroactive NIN collection programme for 28,140 existing accounts.	Engineering and Compliance	**Days 1–5**
3 — CRITICAL	Integrate goAML API for automated STR and CTR generation. Configure ■5,000,000 CTR threshold. Build full submission audit trail.	Engineering	**Days 3–10**
4 — CRITICAL	Deploy AML monitoring platform and connect core transaction feed. Integrate agent network channel on day one of deployment.	CTO and Vendor	**Days 7–21**
5 — HIGH	Engage an independent compliance specialist to produce workpaper-grade evidence, re-performance testing, and the CBN-ready evidence binder required for formal examination.	Board and MLRO	**Immediately**
6 — HIGH	Submit implementation roadmap to the CBN by the 10 June 2026 deadline. This report's 30-day roadmap (Section 07) serves as the foundation.	MLRO and Board	**Before 10 June 2026**

09 COMMITMENT GUARANTEE

[redacted]

IMPORTANT — This is a redacted sample of the executive deliverable produced in StackWeaver's engagements. Workpaper-grade evidence, re-performance testing, transaction sample sizes, and full system-access validation are produced exclusively during the paid engagement with full system access. StackWeaver's Commitment Guarantee applies only to gaps closed under full paid engagement scope. This document does not constitute legal advice.

Reviewed and verified by: Emmanuel O. — Senior Compliance Engineer, 12 years in CBN-regulated financial institutions, AML/CFT specialist, ex-KPMG Advisory, Certified Anti-Money Laundering Specialist (CAMS). · Engagement Reference: SW-2026-CBN-001 · March 2026

stackweaver.cloud · info@stackweaver.cloud · STRICTLY CONFIDENTIAL — Prepared exclusively for NovaPay Financial Technologies Ltd.