FEDERAL MONEY SERVICES BUSINESS ASSOCIATION, VAN YOUNG

Proposal and Comment Information

Title: Request for Information and Comment on Reserve Bank Payment Account Prototype, OP-1877

Comment ID: FR-2025-0083-01-C01

Subject

Re: Docket # OP-1877 - Request for Information and Comment on Reserve Bank Payment Account Prototype

Submitter Information

Organization Name: Federal Money Services Business Association

Organization Type: Organization

Name: Van Young

Submitted Date: 12/22/2025

COVER PAGE
Submitted via: Federal Reserve Board Proposal Comment Process
Re: Request for Information and Comment on Reserve Bank Payment Account Prototype
Docket No.: OP-1877
Commenter: Federal Money Services Business Association (FedMSB)

Date: December 22, 2025

Contact:
Van Young, President
Federal Money Services Business Association (FedMSB)
P.O. Box 5007
Long Island City, NY 11105
Email: govt@fedmsb.org
Phone: 212-951-1168

A formal public comment submission to the Federal Reserve Board's RFI on the Reserve Bank "Payment Account" prototype (Docket OP-1877), submitted by the Federal Money Services Business Association (FedMSB) and signed by its president, Van Young, dated December 22, 2025.

COVER PAGE

Submitted via: Federal Reserve Board Proposal Comment Process

Re: *Request for Information and Comment on Reserve Bank Payment Account Prototype*

Docket No.: OP-1877

Commenter: Federal Money Services Business Association (FedMSB)

Date: December 22, 2025

Contact:

Van Young, President

Federal Money Services Business Association (FedMSB)

P.O. Box 5007

Long Island City, NY 11105

Email: President@FedMSB.org

Phone: 212-951-1168

Submission Package

1. Comment Letter

2. Appendix A — Safeguards (Agreement-Ready) + Alignment Matrix

3. Appendix B — Technical Attachment: Controls / Metrics / Reporting Package (Schema + Validation)
    a. Appendix B-1: Metric Dictionary (Complete) + B-1 Index (New)
    b. Appendix B-2: Materiality Thresholds (Tiered / Relative)
    c. Appendix B-3: Data Quality Controls (Minimum)
    d. Appendix B-4: Submission Checklist (Operator-Ready)

- Footnotes

COMMENT LETTER

To:

The Board of Governors

The Federal Reserve System

20th Street and Constitution Avenue NW

Washington, DC 20551

Re: *Request for Information and Comment on Reserve Bank Payment Account Prototype*

Docket No.: OP-1877

EXECUTIVE "DECISION / ASK" SUMMARY

FedMSB respectfully recommends that the Board and Reserve Banks consider the following actions, within existing statutory and regulatory boundaries:

A) If the Board proceeds with a Payment Account prototype for eligible institutions, the framework should include safeguards that are concrete, auditable, and enforceable, including (i) explicit minimum AML/BSA/CFT and sanctions controls; (ii) independent testing; (iii) standardized periodic reporting with officer attestations; and (iv) an articulated remediation ladder up to service restriction, suspension, or termination for material deficiencies.

(See Appendix A and Appendix B.) [FN-1][FN-8][FN-9][FN-10]

B) Without changing legal eligibility, the Board and Reserve Banks should strengthen resilience and standardize expectations for indirect settlement access arrangements that are already widely used in modern payment participation models (including correspondent settlement), by clarifying baseline expectations for liquidity management, exception handling, auditability, incident reporting, and critical third-party dependencies.

(See Sections IV–VI; templates/metrics in Appendix B.) [FN-2][FN-7]

C) To reduce bespoke review burden and improve comparability, the Board and Reserve Banks should adopt (or encourage) a standardized reporting package schema and minimum validation rules for safeguards monitoring.

(See Appendix B, Sections B-0.1 through B-0.5.) [FN-9][FN-10]

I. EXECUTIVE SUMMARY

The Federal Money Services Business Association (FedMSB) appreciates the Board's decision to request public input on a special-purpose "Payment Account" prototype designed for the express and limited purpose of clearing and settling an institution's payment activity. FedMSB supports efforts to align payments innovation with safety and soundness through a constrained design (e.g., no interest on balances, no access to Federal Reserve credit, and balance caps) and the Board's statement that the prototype would not expand or otherwise change legal eligibility for access to Federal Reserve payments services. [FN-1]

FedMSB also views this RFI as an opportunity to address a structural feature of the U.S. payments ecosystem: MSBs perform essential functions in domestic payments and cross-border remittances, yet settlement access for MSB activity is generally achieved through indirect arrangements with eligible account holders. Indirect settlement pathways can concentrate operational and liquidity dependencies, amplify discontinuity risk when services are withdrawn (including through "de-risking" dynamics), and create inconsistent, duplicative, and opaque compliance expectations across counterparties. As modern rails scale and more activity maps to a small number of settlement points, indirect access arrangements will increasingly shape payment continuity, settlement finality, and the operational resilience of end-to-end payment chains. [FN-2]

Accordingly, our recommendations focus on:

(A) ensuring any Payment Account prototype is accompanied by safeguards that are sufficiently specific, auditable, and enforceable—particularly for AML/BSA/CFT, sanctions, cyber, and operational risk; and

(B) strengthening resilience, transparency, and standardization of indirect access pathways within existing legal eligibility constraints.

II. INTEREST OF FedMSB AND THE MSB SECTOR

FedMSB is an industry association representing Money Services Businesses (MSBs) and the broader payments ecosystem that supports them. MSBs are defined under federal regulations and are subject to Bank Secrecy Act obligations, including the requirement to develop, implement, and maintain an effective AML program reasonably designed to prevent MSBs from being used to facilitate money laundering and the financing of terrorist activities. [FN-3][FN-4][FN-5]

The MSB sector operates at significant scale and reach, including extensive nationwide agent networks, and provides essential financial services to households and small businesses, including remittances and other payment services. [FN-6]

III. LEGAL AND POLICY CONTEXT (BOUNDARY CLARITY AND NON-REQUESTS)

FedMSB is not requesting that the Board alter statutory eligibility for Federal Reserve accounts and services. We acknowledge the Board's statement that a Payment Account would not expand or otherwise change legal eligibility. [FN-1]

FedMSB is also not requesting that the Federal Reserve assume the role of primary AML/BSA/CFT supervisor for MSBs, nor that the Federal Reserve replace FinCEN or OFAC's authorities. Our recommendations instead focus on (i) specifying and enforcing safeguards for any Payment Account prototype made available to legally eligible institutions, and (ii) clarifying baseline expectations for indirect settlement access arrangements already used in the payments ecosystem, consistent with Reserve Bank operational responsibilities and risk management objectives. [FN-7]

IV. RECOMMENDATIONS (SUBSTANCE)

Recommendation 1: If the Payment Account prototype proceeds, adopt supervisory-grade safeguards that are concrete, auditable, and enforceable

FedMSB recommends that any Payment Account framework incorporate minimum safeguards that are:

1. Concrete: defined control requirements and governance,
2. Auditable: independent testing, evidence retention, and standardized metrics, and
3. Enforceable: consequences that scale from remediation to restrictions and, if warranted, suspension/termination.

Appendix A provides an agreement-ready safeguards framework suitable for incorporation into account terms and periodic reporting/attestations. Appendix B provides a standardized controls/metrics/reporting package, with a submission schema and minimum validation rules to support comparability and reduce bespoke review burden. [FN-8][FN-9][FN-10]

Recommendation 2: Strengthen resilience and standardize expectations for indirect settlement access within existing eligibility constraints

Because the Payment Account does not change legal eligibility, a practical near-term objective is to reduce fragility and inconsistency in indirect access arrangements. FedMSB recommends that the Board and Reserve Banks consider clarifying baseline expectations for correspondent/respondent settlement relationships—particularly those supporting participation in modern instant payment rails—covering liquidity management, exception handling, auditability, incident reporting, and critical third-party dependencies. [FN-2]

These steps can improve continuity and risk management without changing legal eligibility, and can reduce duplicative and inconsistent compliance demands by enabling standardized “packages” of controls and reporting appropriate to risk. [FN-7]

V. IMPLEMENTATION AT A GLANCE (30 / 90 / 180 DAYS)

Within 30 days (conceptual to implementable):

- Publish (or outline) a "Safeguards Minimum Set" structure mapped to agreement-ready terms (Appendix A structure).
- Adopt a standard submission package index (Appendix B-0.1) and file naming convention (Appendix B-0.2).
- Specify default reporting cadence (quarterly) and event-driven incident reporting triggers (Appendix B-2).

Within 90 days (pilot-ready documentation):

- Finalize agreement-ready safeguards language (shall/may/breach/remediation ladder).
- Publish submission schema and validation rules (Appendix B-0.3 and B-0.4).
- Pilot the reporting package with a limited set of institutions (or voluntary submissions) to test comparability and burden.

Within 180 days (operationalization):

- Operationalize enhanced reporting and remediation ladder mechanics.
- Provide standardized guidance for indirect access baseline expectations that Reserve Banks and account-holding institutions can adopt consistently.

VI. ANTICIPATED COUNTERARGUMENTS AND RESPONSES

1. "MSBs are not legally eligible for Federal Reserve accounts."

FedMSB is not requesting statutory eligibility changes. Our proposals focus on safeguards for a Payment Account prototype (for eligible institutions) and standardization of indirect settlement arrangements that already exist and are integral to participation in modern payment rails. [FN-1][FN-7]

2. "AML/CFT risk is too high for novel access models."

We agree that safeguards must be explicit and enforceable. Appendix A and B provide a supervisory-grade controls/metrics/reporting and remediation ladder designed to mitigate illicit finance risk through auditable evidence and consequences for material deficiencies. [FN-3][FN-8][FN-9][FN-10]

3. "This creates regulatory arbitrage or weakens supervision."

Standardization with explicit controls, independent testing, attestations, and reporting reduces opacity and improves comparability. Nothing in this package reduces applicable BSA/AML or sanctions obligations; it operationalizes established expectations in a consistent and enforceable way. [FN-3][FN-8][FN-9]

4. "Reserve Banks will face increased operational burden."

A standardized reporting package schema and minimum validation rules reduce burden by improving data structure consistency, enabling comparability, and reducing bespoke review friction and rework. [FN-9][FN-10]

5. "One-size thresholds won't fit all."

Appendix B-2 uses tiered/relative thresholds rather than a single hard number, allowing risk-based calibration while preserving comparability.

VII. RESPONSES TO SELECTED RFI TOPICS

1. Benefits and supported use cases.

A constrained payments-only account may support clearing and settlement needs while reducing credit exposure compared to a broader account construct. [FN-1]

2. Innovation barriers alleviated.

A payments-only construct may mitigate "all-or-nothing" dynamics for eligible institutions seeking only settlement services. [FN-7]

3. Potential risk increases.

Risks rise if AML/BSA/CFT, sanctions, and cyber/operational controls are not verifiable and enforceable, particularly for institutions outside Federal Reserve supervision. [FN-1][FN-3][FN-9][FN-10]

4. Balance cap calibration.

Caps can reduce externalities but should be calibrated to realistic settlement liquidity needs, with transparent compliance mechanics. [FN-1]

5. No interest.

No interest reduces incentives to treat the account as a value storage vehicle. [FN-1]

6. AML/BSA/CFT linkage.

Require concrete controls, independent testing, standardized metrics, and enforceable consequences (Appendices A and B). [FN-3][FN-8][FN-9][FN-10]

7. Other features.

Standardized incident reporting, cyber resilience requirements, third-party risk management, and clarity on permissible integrations and service-provider roles (Appendix B). [FN-10]

VIII. CONCLUSION

FedMSB supports the Board's exploration of a narrowly tailored Payment Account prototype as a potential addition to the access toolkit—provided safeguards are specified with supervisory-grade clarity, auditability, and enforceability. FedMSB also encourages the Board to use this RFI process to strengthen resilience and standardization of indirect access pathways that underpin MSB participation in modern payments, within existing legal eligibility constraints. [FN-1][FN-2][FN-7]

Respectfully submitted,

Van Young

President of FedMSB

Federal Money Services Business Association (FedMSB)

P.O. Box 5007

Long Island City, NY 11105

president@fedmsb.org

212-951-1168

APPENDIX A — SAFEGUARDS

(Supervisory-Grade, Implementable; Suitable for Account Agreement / Attestation / Reporting)

A-0. PURPOSE AND SCOPE

A-0.1 Purpose.

This Appendix sets forth minimum safeguards intended to ensure that any Payment Account (or equivalent payments-only settlement access arrangement) operates with controls that are concrete, auditable, and enforceable, including AML/BSA/CFT and operational/cyber safeguards.

A-0.2 Scope.

These safeguards apply to covered activity (onboarding, messaging, settlement prefunding, exception handling) and to critical vendors supporting the covered activity.

A-1. GOVERNANCE AND ACCOUNTABILITY

A-1.1 Designated Officer.

The Account Holder shall designate a BSA/AML Officer with sufficient authority and independence to design and maintain the AML/BSA/CFT compliance program and to escalate issues to senior management and the board. [FN-3][FN-8]

A-1.2 Board Oversight.

The Account Holder shall obtain board-level approval of the AML/BSA/CFT program and shall conduct an annual effectiveness review, documented in board materials. [FN-3][FN-8]

A-1.3 Training.

The Account Holder shall maintain role-based training with completion tracking for relevant personnel. [FN-8]

A-2. INDEPENDENT TESTING AND AUDITABILITY

A-2.1 Independent Testing.

The Account Holder shall obtain independent testing at least annually (or more frequently based on risk), covering: sanctions screening, transaction monitoring, CDD/KYC, SAR governance, data integrity, and model risk (if applicable). [FN-8][FN-10]

A-2.2 Evidence and Records.

The Account Holder shall maintain records sufficient to support independent testing and Reserve Bank review, consistent with applicable law and regulation, including logs necessary to reconstruct screening results, alerts, investigations, dispositions, and filing decisions. [FN-3][FN-9][FN-10]

A-3. AML/BSA/CFT BASELINE CONTROLS

A-3.1 Risk Assessment.

The Account Holder shall maintain a documented enterprise risk assessment covering products/services, geographies, customer types, delivery channels, transaction velocity, and agent use, and shall update it at least annually and upon material changes. [FN-8][FN-10]

A-3.2 Customer Due Diligence (CDD/EDD).

The Account Holder shall maintain risk-based CDD and enhanced due diligence for higher-risk categories, including periodic refresh cycles and trigger-based reviews. [FN-3][FN-8]

A-3.3 Sanctions Compliance.

The Account Holder shall conduct sanctions screening of customers and relevant counterparties and, where feasible, relevant payment messages, and shall maintain escalation procedures and documented resolution standards. [FN-9]

A-3.4 Transaction Monitoring.

The Account Holder shall maintain risk-based monitoring calibrated to typologies with documented thresholds/scenarios and governance for tuning and change control. [FN-8][FN-10]

A-3.5 SAR/CTR/Recordkeeping Governance.

The Account Holder shall maintain written escalation, investigation, decisioning, and filing procedures, and retention/retrieval controls. [FN-3][FN-8]

A-4. DATA, TECHNOLOGY, AND COMPLIANCE VERIFIABILITY

A-4.1 Data Integrity.

The Account Holder shall maintain controls ensuring completeness and accuracy of data inputs used for sanctions and monitoring, including data lineage documentation and access controls. [FN-10]

A-4.2 Model Risk (if applicable).

Where models/automation are used, the Account Holder shall maintain validation, performance monitoring, and documented approvals for material changes. [FN-10]

A-4.3 System Access Controls.

The Account Holder shall implement MFA and privileged access controls for settlement and compliance systems, with logging and periodic review. [FN-10]

A-5. OPERATIONAL AND CYBER RESILIENCE (SETTLEMENT-CRITICAL)

A-5.1 Incident Response.

The Account Holder shall maintain an incident response plan with severity levels and shall notify the Reserve Bank of material incidents affecting settlement integrity within the timeline specified in the account agreement (default recommended in Appendix B-2). [FN-10]

A-5.2 BCP/DR.

The Account Holder shall test BCP/DR at least annually and maintain RTO/RPO appropriate to settlement operations. [FN-10]

A-5.3 Third-Party Risk.

The Account Holder shall perform due diligence and ongoing monitoring for critical vendors and shall maintain contractual rights sufficient to support auditability and incident response coordination. [FN-10]

A-6. PERIODIC REPORTING, ATTESTATIONS, AND MONITORING

A-6.1 Reporting.

The Account Holder shall submit periodic reporting packages using Appendix B templates, schema, and validation rules (quarterly minimum; more frequent as risk warrants). [FN-9][FN-10]

A-6.2 Officer Attestation.

The Account Holder shall provide an officer certification for each reporting period consistent with Appendix B, Section 7. [FN-9]

A-6.3 Change Log.

The Account Holder shall maintain a program change log for material policy/system/scenario/vendor/staffing changes consistent with Appendix B, Section 6. [FN-9][FN-10]

A-7. REMEDIATION LADDER AND ENFORCEABILITY

A-7.1 Findings and Corrective Action.

Upon identification of a material deficiency, the Account Holder shall provide a corrective action plan (CAP) with timelines and evidence of completion.

A-7.2 Graduated Constraints.

The Reserve Bank may impose graduated constraints for unresolved deficiencies, including: tighter balance limits, service restrictions, enhanced reporting, and additional independent testing.

A-7.3 Material Breach; Suspension/Termination.

Failure to maintain the minimum safeguards, willful blindness, or repeated material deficiencies may constitute a material breach of the account agreement and may result in suspension or termination, consistent with applicable Reserve Bank policies and agreements.

A-8. NO OVERDRAFT / PREFUNDING DISCIPLINE

A-8.1 Liquidity Policy.

The Account Holder shall maintain defined liquidity management policies supporting prefunding and preventing negative positions.

A-8.2 Exception Handling.

The Account Holder shall maintain procedures for rejected payments and exception handling, with approvals logged and reported via Appendix B metrics and change logs.

APPENDIX A-1 — ALIGNMENT MATRIX (CONCEPTUAL; "NOT NOVEL" POSITIONING)

The safeguards above reflect established compliance program components commonly recognized across AML/BSA/CFT and sanctions compliance expectations (risk assessment, internal controls, independent testing, designated compliance officer, training, recordkeeping, and governance), and operational resilience expectations (incident response, BCP/DR, third-party risk management). This Appendix is intended to demonstrate that the safeguards framework is a standardization and enforceability mechanism rather than the creation of novel compliance concepts. [FN-3][FN-8][FN-9][FN-10]

END

APPENDIX B — TECHNICAL ATTACHMENT

Controls / Metrics / Reporting Package (AML/BSA/CFT + Operational Resilience)

Purpose: Provide a supervisory-grade, auditable, enforceable controls/metrics/reporting package with standardized schema and validation rules to improve comparability and reduce bespoke review burden.

B-0. SUBMISSION PACKAGE (INDEX, NAMING, SCHEMA, VALIDATION)

B-0.1 Submission Package Index (What to submit)

Periodic Package (Quarterly default):

A) B0-A Executive Summary (PDF or text): one-page summary of key metrics, incidents, and changes.

B) B0-B Metrics Dataset (CSV/XLSX): required columns in Section 5.2 plus schema in B-0.3.

C) B0-C Program Change Log (CSV/XLSX or text): Section 6 template.

D) B0-D Officer Attestation (signed PDF or text): Section 7 template.

E) B0-E Exceptions Schedule (text/CSV): deviations from Minimum Control Set with remediation status.

F) B0-F Incident/Issue Log (text/CSV): all material incidents and notable issues, cross-referenced to OPS-M metrics.

Event-Driven Package (Material Incident):

A) Material Incident Notification (Section 8 template) submitted within the declared timeline.

B-0.2 File Naming Convention (Recommended)

EntityName_DocketOP-1877_PeriodYYYYQ#_FileType_v#.ext

Examples:

FedMSBMemberCo_OP-1877_2026Q1_Metrics_v1.csv

FedMSBMemberCo_OP-1877_2026Q1_ChangeLog_v1.xlsx

FedMSBMemberCo_OP-1877_2026Q1_Attestation_v1.pdf

B-0.3 Schema (Required columns, types, formatting)

Metrics Dataset (B0-B) columns and types:

- PeriodStart (date, ISO: YYYY-MM-DD)
- PeriodEnd (date, ISO: YYYY-MM-DD)
- MetricID (string, e.g., “SAN-M1”)
- MetricName (string)
- Value (number; integer for counts; decimal allowed for %, $)
- Unit (string enumeration: count | % | hours | days | $ | minutes | date | boolean | text)
- BreakoutType (string enumeration: rail | risk_tier | scenario | scenario_family | product | geo | vendor_system | severity | typology | trigger_type | rationale_category | system_name | planned_unplanned | settlement_model | other)
- BreakoutValue (string)
- Notes (string, optional; max 500 chars recommended)

Formatting requirements:

- Percent values: report as numeric percent (e.g., 12.5 for 12.5%).
- Currency: report in USD unless otherwise specified; if multi-currency, include currency in BreakoutType/Value or Notes.
- Null handling: if Value is unavailable, leave Value blank and explain in Notes; MetricID and Unit must still be present.

B-0.4 Validation Rules (Minimum)

VR-1 Required fields present: PeriodStart, PeriodEnd, MetricID, Value (or Notes explaining blank), Unit.

VR-2 MetricID must match dictionary: MetricID must be one of SAN-M1..SAN-M5, TM-M1..TM-M6, SAR-M1..SAR-M4, CDD-M1..CDD-M5, OPS-M1..OPS-M4, LIQ-M1..LIQ-M5.

VR-3 Unit compatibility:

- Counts must use Unit=count;
- Rates use Unit=%;
- Durations use hours/days/minutes;
- Balances use $.

VR-4 Denominator sanity for rates:

- If a rate is reported, the underlying population counts (e.g., closed cases) should be available somewhere in the same period dataset (may be as a separate Metric row or disclosed in Notes).
- If unavailable, Notes must state why.

VR-5 Time statistic basis:

- Median/percentile metrics must specify whether based on cases closed in period; if not, explain in Notes.

VR-6 Change control traceability:

- Any scenario disabled, threshold changed, vendor swapped, or SLA changed must have a corresponding ChangeLog entry (Section 6).

1. DEFINITIONS AND SCOPE

1.1 Scope of covered activity

Covered activity includes any use of:

- Fedwire Funds, NSS, FedNow, Fedwire Securities Free Transfers (if applicable),

- Any related onboarding, message origination/receipt, liquidity prefunding, exception handling,
- Any third-party service provider functions supporting the above.

1.2 Covered parties

- Account holder (eligible institution requesting/holding a Payment Account)
- Correspondent / settlement agent (if settlement occurs via correspondent master account)
- Respondent / program participant (if applicable)
- Critical vendors (screening, monitoring, messaging, fraud controls, cloud, core systems)

2. CONTROLS CATALOG (MINIMUM CONTROL SET)

Instructions: For each control, provide:

(i) Implemented? (Y/N),

(ii) Owner,

(iii) Evidence reference,

(iv) Last tested date,

(v) Findings/Remediation status.

2.1 Governance & Accountability (GOV)

- GOV-01 Board-approved AML/BSA/CFT policy; annual effectiveness review
- GOV-02 Designated BSA/AML Officer with independence and authority (RACI provided)
- GOV-03 Enterprise risk assessment updated at least annually + event-driven updates
- GOV-04 Independent testing (internal audit or qualified third party) at least annually
- GOV-05 Training program with role-based curricula and completion tracking

Evidence examples: Board minutes, policies, org charts, audit reports, training logs.

2.2 Customer Due Diligence & KYC (CDD)

- CDD-01 Risk-based onboarding KYC procedures (identity, nature of business, expected activity)
- CDD-02 Beneficial ownership/control persons captured where required; verification controls
- CDD-03 EDD triggers and playbooks (high-risk geos, products, typologies)
- CDD-04 Periodic review cadence by risk tier + event triggers (ownership change, anomalies)

2.3 Sanctions Compliance (SAN)

- SAN-01 Sanctions screening at onboarding + documented list update frequency
- SAN-02 Payment message/counterparty screening rules (as data allows)
- SAN-03 Alert escalation standards, false-positive governance, and case documentation
- SAN-04 Blocking/rejecting procedures + reporting workflows

2.4 Transaction Monitoring (TM)

- TM-01 Monitoring scenarios aligned to products/rails (wire, instant, cross-border, cash-in/out)
- TM-02 Scenario tuning governance (change control, approvals, validation)
- TM-03 Investigation SOP (triage → investigate → disposition → SAR decisioning)
- TM-04 Data completeness checks for key fields; lineage documentation
- TM-05 Typology library maintained and reviewed (including terrorist financing indicators)

2.5 SAR / Recordkeeping (SAR)

- SAR-01 SAR governance committee or equivalent escalation path
- SAR-02 Timely filing controls and QA sampling
- SAR-03 Record retention and retrieval controls (audit-ready)
- SAR-04 Law enforcement response procedures (subpoena/314(a)/lawful process)

2.6 Operational & Cyber Resilience (OPS)

- OPS-01 Incident response plan with severity levels; settlement-impact pathway

- OPS-02 BCP/DR tested at least annually; defined RTO/RPO for settlement-critical systems
- OPS-03 Access controls (MFA, privileged access, logging) for settlement and compliance systems
- OPS-04 Third-party risk management for critical vendors (due diligence, SOC reports, audit rights)

2.7 Liquidity / Prefunding Discipline (LIQ)

- LIQ-01 Prefunding policy for rails; intraday liquidity monitoring and limits
- LIQ-02 Rejection handling procedures (failed payments, retries, customer notification)
- LIQ-03 End-of-day controls to remain under overnight balance caps (where applicable)
- LIQ-04 Exception approvals and documentation

3. METRICS & KRIs (LIST + REQUIRED BREAKOUTS)

3.1 Sanctions Screening Metrics (SAN-M)

- SAN-M1 # Sanctions alerts (onboarding)
- SAN-M2 # Sanctions alerts (transactions/messages)
- SAN-M3 Alert-to-case conversion rate (%)
- SAN-M4 Median time-to-close (hours/days)
- SAN-M5 % cases exceeding SLA (e.g., >48h)

Breakouts: by product/rail, risk tier, vendor/system

3.2 Transaction Monitoring Metrics (TM-M)

- TM-M1 # TM alerts generated
- TM-M2 # cases opened
- TM-M3 False positive rate (%)
- TM-M4 Median case age + 95th percentile case age
- TM-M5 # escalations to SAR decisioning
- TM-M6 Scenario health (alerts per scenario; scenarios enabled/disabled)

Breakouts: by scenario family, rail/product, risk tier

3.3 SAR / Reporting Metrics (SAR-M)

- SAR-M1 # SARs filed (count)
- SAR-M2 # SARs by high-level typology (aggregated buckets)
- SAR-M3 Median days from detection to filing decision
- SAR-M4 QA sample size + defect rate (%)

3.4 CDD / EDD Metrics (CDD-M)

- CDD-M1 Total active customers (count)
- CDD-M2 Customers by risk tier (low/med/high)
- CDD-M3 % periodic reviews completed on time
- CDD-M4 # EDD reviews opened/closed; median close time
- CDD-M5 # offboarded for compliance reasons (count)

3.5 Operational Resilience Metrics (OPS-M)

- OPS-M1 # material incidents affecting screening/monitoring/settlement
- OPS-M2 Total downtime minutes (settlement-critical systems)
- OPS-M3 DR test date + pass/fail + key findings
- OPS-M4 # critical vendor incidents and their impact

3.6 Settlement & Liquidity Metrics (LIQ-M)

- LIQ-M1 Average prefunded balance (by rail)
- LIQ-M2 Peak intraday balance (by rail)
- LIQ-M3 # rejected payments due to insufficient funds (count)
- LIQ-M4 # exceptions granted (count) + rationale category
- LIQ-M5 EOD balance compliance rate with cap (if applicable)

NOTE: Definitions, numerators/denominators, and calculation notes are provided in Appendix B-1 (Metric Dictionary).

4. REPORTING CADENCE & DELIVERABLES

4.1 Cadence

- Quarterly package (default)
- Monthly add-on for high-risk profiles or as a condition of approval
- Event-driven reporting within the timeline specified by Appendix B-2

4.2 Deliverables checklist

1. Quarterly Metrics Dashboard (Section 5)
2. Program Change Log (Section 6)
3. Independent Testing Summary (if applicable during the period)
4. Incident Notifications (as triggered)

5. QUARTERLY METRICS DASHBOARD TEMPLATE (FILL-IN)

Reporting period: YYYY-Q#

Entity: [Legal Name]

Settlement model: Direct (Payment Account) / Indirect via correspondent master account

Primary rails used: Fedwire / FedNow / NSS / Securities Free Transfers

5.1 Summary

- Total transaction count: [ ]
- Total transaction value: [ ]
- High-risk share (% by internal risk rating): [ ]
- SARs filed: [ ]
- Material incidents: [ ]

5.2 Detailed metrics file

Format: .xlsx or .csv

Required columns (minimum):

- PeriodStart

- PeriodEnd
- MetricID
- MetricName
- Value
- Unit (count, %, hours, days, $)
- BreakoutType (rail / risk_tier / scenario / scenario_family / product / geo / vendor_system / severity / typology / trigger_type / rationale_category / system_name / planned_unplanned / settlement_model / other)
- BreakoutValue
- Notes (optional)

6. PROGRAM CHANGE LOG TEMPLATE (QUARTERLY)

Required fields:

- ChangeID
- ChangeDate
- ChangeType (policy/system/scenario/vendor/staffing)
- Description
- RiskImpact (low/med/high)
- Approver (name/title)
- Validation performed? (Y/N)
- Backout plan? (Y/N)

7. ATTESTATION TEMPLATE (OFFICER CERTIFICATION)

I, [Name/Title], certify that for the reporting period [dates]:

1. The institution maintained an AML/BSA/CFT compliance program reasonably designed to prevent the institution from being used for money laundering or terrorist financing.

2. The controls listed in the Minimum Control Set (Section 2) were in place, except as disclosed in the Exceptions Schedule attached.
3. Material incidents, control failures, or regulatory inquiries related to illicit finance and settlement integrity were disclosed in the Incident/Issue Log attached.
4. The metrics reported are complete and accurate to the best of my knowledge, and source systems and calculation methodologies are documented and available for review.

Signature: _____ Date: _____

Name/Title: _____

Contact: _____

Attachments required: Exceptions Schedule; Incident/Issue Log.

8. MATERIAL INCIDENT NOTIFICATION TEMPLATE (EVENT-DRIVEN)

Submit within: Per Appendix B-2 recommended timeline (default: within 4 hours of determination of materiality)

Fields:

- IncidentID
- Date/Time detected
- Systems affected (screening/monitoring/settlement/ledger)
- Severity (S1–S4)
- Customer/transaction impact (counts, value, rails)
- Root cause (preliminary)
- Containment actions taken
- Expected resolution time
- Whether suspicious activity may have occurred during control outage (Y/N)
- Post-incident review date + remediation plan

9. REVIEW & ENFORCEMENT HOOKS (OPTIONAL)

Trigger thresholds (examples):

- TM case aging 95th percentile > [X] days for 2 consecutive quarters
- Sanctions SLA breach rate > [Y]%
- Rejected payments due to prefunding failures > [Z] per million
- Two or more S1 incidents in a quarter

Remediation ladder: enhanced reporting → tighter caps/service limits → suspension/termination

==========

APPENDIX B-1 — METRIC DICTIONARY (COMPLETE) + B-1 INDEX (NEW)

B-1 INDEX (Metric Quick Reference)

Sanctions Screening (SAN-M)

- SAN-M1: # Sanctions alerts (onboarding)
- SAN-M2: # Sanctions alerts (transactions/messages)
- SAN-M3: Alert-to-case conversion rate (%)
- SAN-M4: Median time-to-close (hours/days)
- SAN-M5: % cases exceeding SLA (e.g., >48h)

Transaction Monitoring (TM-M)

- TM-M1: # TM alerts generated
- TM-M2: # cases opened
- TM-M3: False positive rate (%)
- TM-M4: Median case age + 95th percentile case age
- TM-M5: # escalations to SAR decisioning
- TM-M6: Scenario health (alerts per scenario; scenarios enabled/disabled)

SAR / Reporting (SAR-M)

- SAR-M1: # SARs filed (count)
- SAR-M2: # SARs by high-level typology (aggregated buckets)
- SAR-M3: Median days from detection to filing decision
- SAR-M4: QA sample size + defect rate (%)

CDD / EDD (CDD-M)

- CDD-M1: Total active customers (count)
- CDD-M2: Customers by risk tier (low/med/high)
- CDD-M3: % periodic reviews completed on time
- CDD-M4: # EDD reviews opened/closed; median close time
- CDD-M5: # offboarded for compliance reasons (count)

Operational Resilience (OPS-M)

- OPS-M1: # material incidents affecting screening/monitoring/settlement
- OPS-M2: Total downtime minutes (settlement-critical systems)
- OPS-M3: DR test date + pass/fail + key findings
- OPS-M4: # critical vendor incidents and their impact

Settlement & Liquidity (LIQ-M)

- LIQ-M1: Average prefunded balance (by rail)
- LIQ-M2: Peak intraday balance (by rail)
- LIQ-M3: # rejected payments due to insufficient funds (count)
- LIQ-M4: # exceptions granted (count) + rationale category
- LIQ-M5: EOD balance compliance rate with cap (if applicable)

B-1 METRIC DICTIONARY (COMPLETE)

A. Global Reporting Conventions (Applies to all metrics)

A1. Reporting window & timezone

- Window: Calendar month or calendar quarter (as specified in the reporting package).
- Timezone: Institution HQ local time; disclose timezone once per package.

A2. De-duplication & identifiers

- Alert de-dupe: Count distinct AlertID per monitoring system.
- Case de-dupe: Count distinct CaseID across systems; if multiple alerts are merged into one case, count one case.
- SAR de-dupe: Count distinct filing (unique SAR submission) in the period.

A3. Case timing

- Case Open timestamp: When a case is created in the case management system.
- Case Close timestamp: When case is dispositioned and closed (not merely "resolved pending QA").
- Age for open cases: If still open at period end, use PeriodEnd as the right endpoint.

A4. SLA declaration

- Any SLA referenced (e.g., ">48h") must be declared in the reporting package header as:

SLA Name / Threshold / Applies to / Effective date.

- Any change must be logged in Program Change Log.

A5. Data quality controls

- Report data completeness exceptions that materially affect monitoring/screening in the Incident/Issue Log and link to OPS-M metrics where relevant.

B. Sanctions Screening Metrics (SAN-M)

SAN-M1 — # Sanctions alerts (onboarding)

- Definition: Count of sanctions screening alerts generated for customer onboarding screening during the reporting period.
- Numerator: Distinct onboarding sanctions AlertID triggered in period.
- Denominator: N/A
- Unit: Count
- Calc Notes: Include initial screening and re-screening triggered during onboarding workflow; exclude batch re-screening of existing customers (report under a separate line item or disclose separately in Notes).

- Primary Data Source: Sanctions screening engine logs + onboarding workflow system.
- Required Breakouts: Product/onboarding channel; risk tier at onboarding; vendor/system.

SAN-M2 — # Sanctions alerts (transactions/messages)

- Definition: Count of sanctions screening alerts generated for transactions and/or payment messages during the reporting period.
- Numerator: Distinct transaction/message sanctions AlertID triggered in period.
- Denominator: N/A
- Unit: Count
- Calc Notes: Include screening on transaction counterparty fields and any message-level screening performed; if message screening is not feasible due to missing data elements, disclose scope limitation in Notes.
- Primary Data Source: Sanctions screening engine logs + payment/rail message store.
- Required Breakouts: Rail (Fedwire/FedNow/NSS/etc.); product; risk tier of originator (if available); vendor/system.

SAN-M3 — Alert-to-case conversion rate (%)

- Definition: Percentage of sanctions alerts that are converted into formal investigation cases.
- Numerator: Distinct sanctions CaseID opened in period with source = sanctions alert(s).
- Denominator: Distinct sanctions AlertID generated in period (SAN-M1 + SAN-M2, unless otherwise specified).
- Unit: Percent (%)
- Calc Notes: If case system batches multiple alerts into one case, numerator is cases; denominator is alerts—this is intended (conversion intensity).
- Primary Data Source: Case management system + sanctions engine crosswalk table.
- Required Breakouts: Rail (where applicable); risk tier; vendor/system.

SAN-M4 — Median time-to-close (hours/days)

- Definition: Median elapsed time from case open to case close for sanctions cases closed in the period.

- Numerator/Denominator: N/A (distribution statistic).
- Unit: Hours or days (declare unit)
- Calc Notes: Compute on cases closed in the period (not opened). Use CaseClose − CaseOpen. Exclude cases that were reopened; if reopened, treat as a new lifecycle or disclose approach.
- Primary Data Source: Case management timestamps.
- Required Breakouts: Rail/product; risk tier; vendor/system.

SAN-M5 — % cases exceeding SLA (e.g., >48h)

- Definition: Percentage of sanctions cases whose time-to-close exceeded the declared SLA threshold.
- Numerator: # sanctions cases closed in period with (CaseClose − CaseOpen) > SLA.
- Denominator: # sanctions cases closed in period.
- Unit: Percent (%)
- Calc Notes: SLA must be defined per A4. If different SLAs by severity, compute separate rows by BreakoutType = severity.
- Primary Data Source: Case management timestamps + SLA parameter table.
- Required Breakouts: Severity tier (if used); rail/product; risk tier; vendor/system.

C. Transaction Monitoring Metrics (TM-M)

TM-M1 — # TM alerts generated

- Definition: Count of transaction monitoring alerts generated in the period.
- Numerator: Distinct TM AlertID generated in period.
- Denominator: N/A
- Unit: Count
- Calc Notes: Include alerts from rules/scenarios and model-based detection; exclude system health/test alerts (flag separately).
- Primary Data Source: TM engine logs.
- Required Breakouts: Rail/product; scenario family; risk tier; vendor/system.

TM-M2 — # cases opened

- Definition: Count of investigation cases opened from TM alerts in the period.
- Numerator: Distinct TM CaseID opened in period with source = TM alert(s).
- Denominator: N/A

- Unit: Count
- Calc Notes: If multiple alerts roll into one case, count one case; linkages should be documented.
- Primary Data Source: Case management system.
- Required Breakouts: Rail/product; scenario family; risk tier; vendor/system.

TM-M3 — False positive rate (%)

- Definition: Percentage of TM cases closed in the period that are dispositioned as "no suspicious activity / no escalation / false positive."
- Numerator: # TM cases closed in period with disposition category = false positive (or equivalent).
- Denominator: # TM cases closed in period.
- Unit: Percent (%)
- Calc Notes: Disposition taxonomy must be provided; if "inconclusive" exists, report separately or define mapping.
- Primary Data Source: Case management disposition fields.
- Required Breakouts: Scenario family; rail/product; risk tier.

TM-M4 — Median case age + 95th percentile case age

- Definition: Median and 95th percentile of elapsed time from case open to case close for TM cases closed in period.
- Unit: Days or hours (declare unit)
- Calc Notes: Compute two statistics over the same closed-case population; for open cases, do not include here (track separately if desired).
- Primary Data Source: Case management timestamps.
- Required Breakouts: Scenario family; rail/product; risk tier.

TM-M5 — # escalations to SAR decisioning

- Definition: Count of TM cases that escalated to SAR decisioning stage in the period.
- Numerator: Distinct TM CaseID with stage transition to "SAR decisioning" (or equivalent) in period.
- Denominator: N/A
- Unit: Count
- Calc Notes: If SAR decisioning occurs after case closure in a separate workflow, use the timestamp when decisioning was initiated.

- Primary Data Source: Case management workflow logs / stage history.
- Required Breakouts: Scenario family; rail/product; risk tier.

TM-M6 — Scenario health (alerts per scenario; scenarios enabled/disabled)

- Definition: Operational statistics per scenario capturing alert volume and whether a scenario is enabled/disabled during the period.
- Numerator:
    - Alerts per scenario = # distinct AlertID for scenario in period
    - Disabled indicator = Y/N (or % of period disabled)
- Denominator: N/A
- Unit: Count (alerts) + Boolean/percent (enabled status)
- Calc Notes: For "partially disabled," report % of period disabled. Any disabling must be in Program Change Log with approvals.
- Primary Data Source: TM engine configuration repository + TM logs.
- Required Breakouts: Scenario ID/name; scenario family; rail/product (if scenario-specific).

D. SAR / Reporting Metrics (SAR-M)

SAR-M1 — # SARs filed (count)

- Definition: Number of SAR filings submitted during the reporting period.
- Numerator: Distinct SAR submissions made in period.
- Denominator: N/A
- Unit: Count
- Calc Notes: Count by filing date (submission timestamp), not by detection date. If amended SARs exist, count them separately or tag as "amended."
- Primary Data Source: SAR filing system / internal submission logs.
- Required Breakouts: High-level typology bucket (if available); product/rail (where attributable).

SAR-M2 — # SARs by high-level typology (aggregated buckets)

- Definition: SAR counts categorized into pre-defined typology buckets.
- Numerator: Distinct SAR filings in period in each typology bucket.
- Denominator: N/A
- Unit: Count

- Calc Notes: Typology taxonomy must be stable; changes must be logged. Multiple typologies per SAR: choose primary typology or allow multi-tag and disclose rule.
- Primary Data Source: SAR case system typology fields.
- Required Breakouts: Typology bucket; product/rail (if available).

SAR-M3 — Median days from detection to filing decision

- Definition: Median elapsed days from initial detection timestamp to SAR filing decision timestamp for SAR-related cases with decisions in period.
- Numerator/Denominator: N/A (distribution statistic).
- Unit: Days
- Calc Notes: “Detection” must be defined (first alert time, case open time, or first internal escalation). Declare chosen source in Notes and apply consistently.
- Primary Data Source: Case workflow timestamps + SAR decisioning logs.
- Required Breakouts: Typology bucket; product/rail (if available).

SAR-M4 — QA sample size + defect rate (%)

- Definition: Quality assurance coverage and defect rate for SAR-related QA reviews performed in period.
- Numerator: # QA reviews with material defects found.
- Denominator: # QA reviews performed in period.
- Unit: Count (sample size) + Percent (%)
- Calc Notes: Define “material defect” categories; report sample selection method (random/risk-based).
- Primary Data Source: QA tracking system / audit workpapers.
- Required Breakouts: Defect category; typology (if applicable).

E. CDD / EDD Metrics (CDD-M)

CDD-M1 — Total active customers (count)

- Definition: Count of active customers at period end (or period average, if specified).
- Numerator: Distinct active CustomerID.
- Denominator: N/A
- Unit: Count
- Calc Notes: Define “active” (open account, not offboarded, not dormant beyond threshold). Disclose definition.
- Primary Data Source: Customer master / CRM / core ledger.

- Required Breakouts: Product line; risk tier.

CDD-M2 — Customers by risk tier (low/med/high)

- Definition: Distribution of active customers by internal risk tier at period end.
- Numerator: Distinct active CustomerID in each tier.
- Denominator: Total active customers (CDD-M1).
- Unit: Count and/or Percent (%) (disclose which)
- Calc Notes: Risk tier methodology changes must be logged.
- Primary Data Source: Risk rating system + customer master.
- Required Breakouts: Product line; geography (optional if used internally).

CDD-M3 — % periodic reviews completed on time

- Definition: Percentage of required periodic reviews due in the period that were completed by the due date.
- Numerator: # periodic reviews completed on/before due date in period.
- Denominator: # periodic reviews due in period.
- Unit: Percent (%)
- Calc Notes: If reviews were completed late, they count as not on time even if completed within grace period (unless grace is declared and consistently used).
- Primary Data Source: CDD/EDD workflow tool.
- Required Breakouts: Risk tier; product line.

CDD-M4 — # EDD reviews opened/closed; median close time

- Definition: Counts of EDD reviews opened and closed in period, plus median close time for EDD reviews closed in period.
- Numerator:
    - Opened = # distinct EDD CaseID opened in period
    - Closed = # distinct EDD CaseID closed in period
    - Median close time = median(CaseClose − CaseOpen) for closed EDD cases
- Denominator: N/A
- Unit: Count + Days (or hours)
- Calc Notes: EDD case definition must be consistent.
- Primary Data Source: EDD case system/workflow.
- Required Breakouts: Trigger type (e.g., high-risk geo, PEP, unusual activity); risk tier.

CDD-M5 — # offboarded for compliance reasons (count)

- Definition: Number of customers exited/terminated for compliance-related reasons in period.
- Numerator: Distinct CustomerID offboarded in period with exit reason = compliance (taxonomy-defined).
- Denominator: N/A
- Unit: Count
- Calc Notes: Provide exit reason taxonomy; if multiple reasons, choose primary reason rule.
- Primary Data Source: Offboarding workflow + customer master.
- Required Breakouts: Product line; risk tier; primary compliance reason category.

F. Operational Resilience Metrics (OPS-M)

OPS-M1 — # material incidents affecting screening/monitoring/settlement

- Definition: Count of incidents meeting the institution's declared materiality thresholds that affected sanctions screening, transaction monitoring, and/or settlement operations during the period.
- Numerator: Distinct IncidentID meeting "material" criteria in period.
- Denominator: N/A
- Unit: Count
- Calc Notes: Materiality thresholds must be declared (see Appendix B-2). If incident spans periods, count in the period it was declared material; reference continuation in Notes.
- Primary Data Source: Incident management system (ITSM/SOC) + compliance incident log.
- Required Breakouts: Impacted domain (screening/monitoring/settlement/ledger); severity (S1–S4); root cause category.

OPS-M2 — Total downtime minutes (settlement-critical systems)

- Definition: Total minutes of unplanned downtime for settlement-critical systems during the period.
- Numerator: Sum of downtime minutes across settlement-critical systems in period.
- Denominator: N/A
- Unit: Minutes
- Calc Notes: Define "downtime" (loss of service, degraded performance beyond threshold). Exclude planned maintenance; report planned separately if desired.

- Primary Data Source: Monitoring/observability platform + incident records.
- Required Breakouts: System name; rail impacted; planned vs unplanned.

OPS-M3 — DR test date + pass/fail + key findings

- Definition: Disaster recovery (DR) test status and outcomes for the period.
- Numerator/Denominator: N/A
- Unit: Date + Boolean + Text summary
- Calc Notes: At minimum include one test per year; include scope and RTO/RPO achieved.
- Primary Data Source: DR test reports / BCP documentation.
- Required Breakouts: System group (settlement, screening, monitoring); test type (tabletop vs failover).

OPS-M4 — # critical vendor incidents and their impact

- Definition: Count of incidents attributable to critical vendors and summary of impacts.
- Numerator: Distinct vendor-related IncidentID in period for vendors classified as "critical."
- Denominator: N/A
- Unit: Count + impact fields (minutes, transactions affected, $ value if known)
- Calc Notes: Critical vendor list must be maintained; changes logged.
- Primary Data Source: Vendor management + incident system.
- Required Breakouts: Vendor name; affected domain; severity.

G. Settlement & Liquidity Metrics (LIQ-M)

LIQ-M1 — Average prefunded balance (by rail)

- Definition: Average prefunded balance maintained for settlement purposes by rail during the period.
- Numerator: Sum of end-of-interval balances (e.g., daily EOD or hourly snapshots) for the rail.
- Denominator: Number of intervals.
- Unit: Dollars ($)
- Calc Notes: Declare sampling interval (daily EOD recommended for quarterly reporting; hourly optional for high-frequency rails).
- Primary Data Source: Settlement ledger / treasury liquidity system.

- Required Breakouts: Rail; settlement model (direct vs correspondent); currency (if multi-currency exists).

LIQ-M2 — Peak intraday balance (by rail)

- Definition: Maximum intraday prefunded balance observed per rail during the period.
- Numerator: Max(balance snapshots) for the rail in period.
- Denominator: N/A
- Unit: Dollars ($)
- Calc Notes: Sampling interval must be disclosed; use highest-resolution available consistently.
- Primary Data Source: Liquidity monitoring system / ledger snapshots.
- Required Breakouts: Rail; date of peak (include in Notes).

LIQ-M3 — # rejected payments due to insufficient funds (count)

- Definition: Number of payment attempts rejected due to insufficient prefunded liquidity during the period.
- Numerator: Distinct payment/message IDs rejected with reason code “insufficient funds/prefunding shortfall.”
- Denominator: N/A
- Unit: Count
- Calc Notes: Separate rejections due to other reasons (format, sanctions block, duplicate) and do not include here.
- Primary Data Source: Rail gateway logs + payment orchestration logs.
- Required Breakouts: Rail; product; reason sub-code (if any).

LIQ-M4 — # exceptions granted (count) + rationale category

- Definition: Number of exceptions granted to standard liquidity/prefunding controls during the period, with categorized rationales.
- Numerator: Distinct exception approvals (ExceptionID) in period.
- Denominator: N/A
- Unit: Count
- Calc Notes: Exception taxonomy must be defined (e.g., operational error, customer urgency, system outage workaround).
- Primary Data Source: Exception approval workflow + treasury operations logs.

- Required Breakouts: Rail; rationale category; approver seniority level (optional).

LIQ-M5 — EOD balance compliance rate with cap (if applicable)

- Definition: Percentage of days in the period where end-of-day (EOD) balance complied with the applicable balance cap.
- Numerator: # days in period with EOD balance ≤ cap.
- Denominator: # days in period.
- Unit: Percent (%)
- Calc Notes: If cap varies (e.g., temporary tighter cap), use the cap effective that day; cap changes must be in Program Change Log.
- Primary Data Source: Ledger EOD balances + cap parameter table.
- Required Breakouts: Settlement model; rail (if caps are rail-specific).

Appendix B-1 Attachment Format (Recommended)

To facilitate review, include a structured Metric Dictionary file (CSV/XLSX) with columns:

MetricID, MetricName, Definition, Numerator, Denominator, Unit, CalculationNotes, PrimaryDataSource, RequiredBreakouts

==========

APPENDIX B-2 — MATERIALITY THRESHOLDS (TIERED / RELATIVE)

Goal: Avoid one-size thresholds while preserving comparability. Institutions should declare their chosen tier and baseline volumes/values each period.

B-2.1 Default notification timeline (recommended)

- Material incident notification: within 4 hours of materiality determination (event-driven).
- Follow-up written update: within 24 hours if initial notice is incomplete.

B-2.2 Tiering approach (choose one tier per period, disclosed in package header)

Tier selection basis (choose one and disclose):

- Average daily settlement transaction count (ADTC), or
- Average daily settlement value (ADSV), or
- Total assets (if available), or
- Another objective scale measure (disclose).

Tier 1 (lower scale)

Treat as material if any of the following occurs:

- Settlement-critical outage ≥ 30 minutes, OR
- Affects ≥ max(25 transactions, 0.5% of ADTC), OR
- Affects ≥ max($250,000, 0.5% of ADSV), OR
- Sanctions/TM control outage ≥ 60 minutes, OR
- Data integrity failure impacting screening/monitoring/settlement with key-field missingness/mismatch ≥ 1.0% (validated sample)
- Cyber/unauthorized access to settlement or compliance systems causing control failure
- Critical vendor incident causing any of the above

Tier 2 (mid scale)

Treat as material if any of the following occurs:

- Settlement-critical outage ≥ 20 minutes, OR
- Affects ≥ max(100 transactions, 0.25% of ADTC), OR
- Affects ≥ max($1,000,000, 0.25% of ADSV), OR
- Sanctions/TM control outage ≥ 45 minutes, OR
- Data integrity failure threshold same as Tier 1 unless justified otherwise
- Cyber/unauthorized access causing control failure
- Critical vendor incident causing any of the above

Tier 3 (higher scale)

Treat as material if any of the following occurs:

- Settlement-critical outage ≥ 10 minutes, OR
- Affects ≥ max(500 transactions, 0.10% of ADTC), OR
- Affects ≥ max($10,000,000, 0.10% of ADSV), OR

- Sanctions/TM control outage ≥ 30 minutes, OR
- Data integrity failure threshold same as Tier 1 unless justified otherwise
- Cyber/unauthorized access causing control failure
- Critical vendor incident causing any of the above

Disclosure requirement:

The reporting package header must disclose the tier basis and ADTC/ADSV baseline used for the period, and any changes must be recorded in the Program Change Log.

==========

APPENDIX B-3 — DATA QUALITY CONTROLS (MINIMUM)

Minimum requirements:

- Reconciliation: Daily reconciliation between settlement ledger and rail reporting/notifications; exceptions triaged within T+1 business day.
- Lineage & Access: Data lineage documentation for key fields + least-privilege access controls with audit logs.
- Change Control: Any change affecting screening/monitoring/settlement parameters, thresholds, or mapping rules must be recorded in the Program Change Log with approvals and backout plan.
- Sampling Discipline: Where thresholds rely on sampling (e.g., key-field mismatch), disclose sampling method, sample size, and confidence constraints in Notes.

==========

APPENDIX B-4 — SUBMISSION CHECKLIST (OPERATOR-READY)

Before submission, confirm:

1. Cover Page complete (date, docket, contact).
2. Comment Letter includes Executive “Decision/Ask” Summary, Implementation timeline, Counterarguments sections.
3. Appendix A included and formatted; remediation ladder present.
4. Appendix B package includes: Summary, Metrics Dataset, Change Log, Attestation, Exceptions Schedule, Incident/Issue Log.
5. Metrics Dataset passes VR-1 to VR-6 validation rules (or exceptions explained in Notes).
6. Tier basis and baseline (ADTC/ADSV or other) disclosed for Appendix B-2.
7. All material incidents have Section 8 notifications logged and cross-referenced in OPS-M metrics.
8. All scenario/threshold/SLA changes appear in Change Log with approvals and backout plans.

END

FOOTNOTES

[FN-1] Board of Governors of the Federal Reserve System (Issuer), "Federal Reserve Board requests public input on 'payment account,' which eligible financial institutions could use for the limited purpose of clearing and settling their payments" (Press Release), Dec. 19, 2025 (topic: Payment Account concept; constraints including no interest, no Fed credit, balance caps; statement that it would not expand or otherwise change legal eligibility; includes accompanying statements).

URL: https://www.federalreserve.gov/newsevents/pressreleases/bcreg20251219a.htm

[FN-2] Federal Reserve Financial Services (Issuer), FedNow Service documentation (topic: settlement constructs; mapping to a settlement account/settlement point; participation models including correspondent settlement).

URL: https://www.frbservices.org/financial-services/fednow

[FN-3] Financial Crimes Enforcement Network (FinCEN) (Issuer), 31 CFR 1022.210 (topic: anti-money laundering programs for money services businesses; "reasonably designed" AML program requirement).

URL: https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1022/section-1022.210

[FN-4] Financial Crimes Enforcement Network (FinCEN) (Issuer), 31 CFR 1010.100(ff) (topic: definition of "money services business" and scope).

URL: https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X/part-1010/section-1010.100

[FN-5] Bank Secrecy Act / FinCEN regulatory framework (topic: general AML/BSA/CFT reporting and recordkeeping structure as implemented through FinCEN regulations applicable to MSBs; referenced for contextual completeness).

URL (general eCFR Title 31, Chapter X entry point): https://www.ecfr.gov/current/title-31/subtitle-B/chapter-X

[FN-6] Financial Crimes Enforcement Network (FinCEN) Federal Register notices and public materials (topic: MSB registration/agent network scale; general public references

discussing agent MSB counts and registration program operations; cited for sector context).

URL (FinCEN Federal Register landing page for agency documents): https://www.federalregister.gov/agencies/financial-crimes-enforcement-network

[FN-7] Board of Governors of the Federal Reserve System (Issuer), "Guidelines for Evaluating Account and Services Requests" (topic: risk-based evaluation considerations including legal eligibility, supervision, and other risk factors).

URL: https://www.federalreserve.gov/newsevents/pressreleases/other20220815a.htm

[FN-8] Federal Financial Institutions Examination Council (FFIEC) (Issuer), "BSA/AML Examination Manual" (topic: core program pillars and supervisory expectations; risk assessment, internal controls, independent testing, BSA officer, training; governance and related expectations).

URL: https://bsaaml.ffiec.gov/

[FN-9] U.S. Department of the Treasury, Office of Foreign Assets Control (OFAC) (Issuer), "A Framework for OFAC Compliance Commitments" (topic: essential sanctions compliance elements: management commitment, risk assessment, internal controls, testing/auditing, training).

URL: https://ofac.treasury.gov/media/16386/download?inline

[FN-10] General financial sector supervisory expectations and widely adopted risk management practices (topic: operational resilience, incident response, BCP/DR, third-party risk management; included as contextual support for the operational resilience elements of Appendix A/B).

****Note:*** This citation is intentionally general and does not assert a single controlling document; it reflects common supervisory and industry practice across U.S. financial sector guidance.