Enterprise-Wide Global AML Program

This document is the Firm's **written AML compliance program** for the purposes of 31 CFR § 1020.210 and the equivalent requirements applying to each regulated Northgate entity. It describes, in one place, how the Firm is organised to prevent, detect and report money laundering and terrorist financing across every legal entity, business and jurisdiction in which it operates — who is accountable, what each component of the program does, how the components connect, how the program is resourced and tested, and how the Board satisfies itself that it works. It was approved by the Board of Directors and the approval is recorded in the minutes.

Document control	Detail
Document title	Enterprise-Wide Global AML Program
Statutory status	The written program required by 31 CFR § 1020.210; the AML compliance program required of Northgate Securities LLC under FINRA Rule 3310 and 31 CFR § 1023.210; and the group-wide program required under applicable non-US regimes
Version	9.0
Owner	Global Head of Financial Crimes Compliance, designated BSA/AML Officer
Approved by	Board of Directors, 12 March 2026, on the recommendation of the Risk Committee and the Audit Committee; recorded in the minutes of that meeting
Effective date	1 April 2026; reapproved by the Board at least annually
Scope	14 legal entities; 9 business lines; 4 regions; 38 jurisdictions of operation
Program headcount	1,410 FTE in Financial Crimes Compliance, plus 620 FTE in first-line financial-crime operations (see § 12)
Constituent documents	Global AML Policy (L1); AML Control Framework and RCM (L2); EWRA Methodology (L2); Global AML Operating Procedures (L3); Global Sanctions Policy and Framework; Country Risk Methodology; Model Risk Management Policy; AML Training Curriculum; Independent Testing Plan

Illustrative training specimen. "Northgate Financial Group, Inc." is a fictional institution created for instructional use. This document is modelled on the structure, register and technical content of a US Category I bank holding company financial-crime document set and is not the document of any real firm. Thresholds, cycle times and tolerances shown are representative and must not be read as regulatory minimums except where a statutory citation is given.

Contents

1. Board statement and program summary

> **Statement of the Board of Directors**
>
> The Board of Directors of Northgate Financial Group, Inc. has approved this Enterprise-Wide Global AML Program. The Board is accountable for the Program. It has appointed a qualified BSA/AML Officer, has satisfied itself that the Officer is independent, sufficiently senior and adequately resourced, and has established the reporting lines and committee structures necessary for the Board to hold management to account. The Board expects the Program to be effective in practice, not merely compliant in form, and will assess it on that basis. Where the Program is found wanting, the Board expects to be told promptly, in writing, without softening, and by the BSA/AML Officer directly.

1.1 What the Program is

The Program is the sum of the Firm’s people, governance, policies, controls, systems, data and assurance dedicated to preventing the Firm from being used to launder money or finance terrorism. It is organised into seven components, each described in this document, and each connected to the others by design:

Component	Purpose	Detail in
1. Risk assessment	Establish, on evidence, where the Firm's ML/TF risk actually sits, and drive everything else from it.	§ 7 and the EWRA Methodology (L2)
2. Customer due diligence and screening	Know who the Firm is dealing with, before it deals with them, and keep knowing.	§ 8
3. Detection, investigation and reporting	Identify unusual activity, investigate it, and report suspicion to the authorities.	§ 9
4. Training and awareness	Ensure every person who can see risk knows what to do about it.	§ 10
5. Independent testing and assurance	Establish independently whether the Program actually works.	§ 10
6. Technology, data and models	Provide the detection capability the Program depends on, and govern it.	§ 11
7. Governance, culture and accountability	Ensure decisions are made by the right people, for the right reasons, and that escalation is safe.	§ 4 and the Global AML Policy (L1)

1.2 The Firm's current position, in summary

The 2025 EWRA concluded that the Firm's enterprise residual ML/TF risk is **Moderate**, with three assessment units carrying High or Very High residual risk: correspondent banking in EMEA; private banking in APAC; and digital-asset services globally. Action plans are in place for each, with named owners, funded remediation, interim compensating controls and Board oversight. The Firm has no open Critical AML issues and two open Matters Requiring Attention, both within their agreed remediation timelines. The BSA/AML Officer's opinion, stated to the Board, is that the Program is effective, with the identified exceptions, and that the resources requested for 2026 are adequate to the risk.

2. The regulated perimeter: entities, regulators and program applicability

The Firm operates a **single global Program**, applied to every entity. Individual entities may sit under different regulators with different statutory program requirements; the Program is designed so that each entity meets its own requirements while operating one coherent set of standards. Where a local requirement is stricter, the stricter requirement applies locally; the global standard is never the ceiling. See § 13.

Fourteen legal entities are in scope. The principal entities and their prudential and conduct regulators are set out in Appendix A. Each regulated entity has a designated local AML officer or Money Laundering Reporting Officer who reports functionally to the BSA/AML Officer and holds equivalent local independence, authority, access and protection.

> **One Program, many regulators**
>
> The most common failure mode in a multinational group is not that a jurisdiction is ignored — it is that each jurisdiction builds its own program, and the group ends up with fourteen programs, fourteen risk assessments, fourteen sets of thresholds, and no one able to answer the question 'what is our exposure to this typology across the Firm?' The Program is deliberately singular for that reason. Local addenda raise the standard for local requirements; they do not fork the Program.

3. Program architecture and document hierarchy

Level	Document	Approved by	Answers
L1	Global AML Policy	Board of Directors	What must be true, what is prohibited, and who is accountable
L1	Global Sanctions Policy	Board of Directors	Sanctions obligations — strict liability, distinct from the risk-based AML regime
L2	AML Control Framework and Risk-Control Matrix	BSA/AML Officer	Which controls exist, what each must achieve, who owns it, how it is tested
L2	EWRA Methodology and Procedures	BSA/AML Officer; validated by Model Risk	How the Firm establishes what its risk is
L2	Country Risk Methodology	BSA/AML Officer	How jurisdictions are rated, and what a rating drives
L3	Global AML Operating Procedures	Head of FC Operations	Who does what, in what order, by when, with what evidence
L3	Local addenda (per jurisdiction)	Local MLRO, concurred by FCC	Additional local requirements that raise the standard
L4	System work instructions and job aids	Team leads	Which button to press
—	**This document**	Board of Directors	How all of the above fits together, is resourced, and is proved to work

Where any document conflicts with a higher level, the higher level prevails, and the conflict must be reported to the owner of the higher-level document within one business day of discovery. There is no fifth level: an instruction that is not traceable to this hierarchy is not a Firm requirement and must not be followed.

4. Governance: Board, committees and management bodies

Body	Cadence	Mandate in respect of the Program	Escalates to
Board of Directors	Quarterly (AML standing item); annually for Program approval	Approves the Program, the Policy, the risk appetite and the EWRA. Appoints and, if necessary, removes the BSA/AML Officer. Holds management to the remediation of findings. Sets the tone.	—
Risk Committee of the Board	Bi-monthly	Oversees financial-crime risk as a component of non-financial risk. Receives a standing report from the BSA/AML Officer at every meeting. Reviews appetite breaches and material risk acceptances.	Board
Audit Committee of the Board	Quarterly	Oversees the independence, scope and adequacy of independent testing. Monitors closure of audit and examination findings. Receives the Chief Audit Executive unfiltered.	Board
Financial Crimes Risk Committee	Monthly	The senior executive forum. Reviews the aggregate risk profile; decides the highest-risk relationships; approves the Restricted Business Schedule and the Country Risk List; reviews thematic findings and remediation; decides contested exits. Chaired by the BSA/AML Officer.	Risk Committee
SAR Review Committee	Twice weekly, plus ad hoc	Decides whether to file. No business representative attends and no commercial information is presented to it.	BSA/AML Officer
Model Risk Committee	Quarterly	Governs the validation of NG-DETECT, the NG-KYC rating model and the EWRA methodology.	Risk Committee

Body	Cadence	Mandate in respect of the Program	Escalates to
Regional / entity financial crime committees	Monthly	Local execution, local risk, local regulatory relationships. Functionally accountable to the Financial Crimes Risk Committee — not to the local business head.	Financial Crimes Risk Committee

4.1 What the Board actually receives

The Board is entitled to information sufficient to **challenge**, not merely to note. The mandatory contents of the quarterly Board pack are in Appendix C. Reporting must be accurate, timely and complete, and must present adverse trends as adverse. No business may filter, soften or delay financial-crime management information, and the BSA/AML Officer owns its integrity.

5. The BSA/AML Officer and the FCC organisation

The Board has designated the Global Head of Financial Crimes Compliance as the Firm's BSA/AML Officer under 31 CFR § 1020.210. The conditions of the role — independence, access, authority, resourcing, protection and removal only by the Board with notification to the Firm's primary federal regulators — are set out in § 7 of the Global AML Policy and are not repeated here. They are conditions of the Program, not privileges of the individual.

5.1 The FCC organisation

Function	Reports to	Accountable for	FTE
FCC Advisory	Global Head of FCC	Policy interpretation; EDD and restricted business approval; the right to decline and to exit; regulatory interpretation; 314(a)/(b).	185
FC Risk and Control	Global Head of FCC	The EWRA; the AML Control Framework and RCM; scenario and threshold governance; the KRI framework; control testing coordination.	140
FC Investigations	Global Head of FCC	Alert investigation (L2/L3); case management; the SAR Review Committee; law-enforcement liaison.	480
Screening Operations	Global Head of FCC	PEP and adverse-media match disposition; list management (jointly with Sanctions).	150
Regulatory Reporting	Global Head of FCC	SAR, CTR, 314(a) and blocked-property filing; acknowledgement reconciliation; filing timeliness.	95
Sanctions Compliance	Global Head of FCC (Global Sanctions Officer)	Sanctions determinations; blocking and rejection; OFAC reporting and licensing. Governed by the Sanctions Framework; interfaces with this Program at § 8.4.	165
FC Technology and Data	Global Head of FCC (matrixed to the CIO)	NG-DETECT, NG-SCREEN, NG-KYC, NG-CASE, NG-FILE; data coverage, quality and lineage.	120
Quality Assurance	Head of FC Operations	Independent post-completion sampling of every decision type; error grading; theme reporting.	75
Compliance Testing and Monitoring (CTM)	Chief Compliance Officer (independent of FCC operations)	2LOD testing of the design and operating effectiveness of every Key Control.	N/A — sits in Co mpliance

Why CTM does not report to FCC operations

A testing function that reports to the people whose work it tests will, over time, test less and find less. CTM sits under the Chief Compliance Officer, outside the FCC operational reporting line, precisely so that it can conclude that a control operated by FCC is not effective — and so that Internal Audit can rely on it. Where 2LOD testing reports into 2LOD operations, Internal Audit will not rely on it, and the cost of assurance doubles.

6. The statutory pillars, and how the Firm evidences each

Pillar	How the Firm satisfies it	Evidence an examiner will be shown
Internal controls, policies and procedures	The Global AML Policy (L1), the AML Control Framework and RCM (L2, 68 controls, 24 designated Key), and the Global AML Operating Procedures (L3).	The RCM in NG-GRC; control detail sheets; the annual control attestation by every control owner; the exceptions and deviation registers.
Designated compliance officer	The BSA/AML Officer, appointed by the Board, independent of the businesses, with no revenue responsibility, direct Board access, and authority to decline, restrict, exit and file without business consent.	The Board minute of appointment; the reporting line; the Board pack showing direct reporting; the record of declines and exits over business objection.
Ongoing employee training	Mandatory annual training for all staff and directors; role-specific training for higher-risk roles; assessed comprehension, not attendance.	Completion MI (99.4% for 2025); assessment pass rates by cohort; the curriculum traced to the EWRA and the national priorities; the access-suspension log for non-completers.
Independent testing	Internal Audit, reporting to the Audit Committee, with the AML program in permanent scope; supplemented by external specialists where Internal Audit lacks the expertise; supported by 2LOD CTM testing that Internal Audit assesses before relying on.	The audit plan risk-ranked against the EWRA; the audit reports; the finding tracker; the Audit Committee minutes; the validation of closed findings.
Customer due diligence	Risk-based CIP, beneficial ownership, KYC profile, risk rating, EDD and ongoing monitoring, per the Operating Procedures.	NG-KYC records; the risk-rating model and its validation; the override register; the periodic review ageing; the QA sampling results.
Effectiveness and risk-based prioritisation (AMLA 2020)	The EWRA drives resourcing, scenarios, thresholds, training and testing. The national priorities are assessed by name. The Firm measures whether the Program works, not whether it exists (§ 14).	The EWRA and its traceability matrix; the KRI dashboard; the effectiveness self-assessment; the Board pack.

7. Program component: Enterprise-Wide Risk Assessment

The EWRA is the foundation of the Program and is described in full in the EWRA Methodology and Procedures (L2). In summary: inherent risk is scored across five factor categories (customers, products, geographies, channels, transactions) against binding, data-anchored scoring anchors; control effectiveness is derived from testing results, open issues, audit and examination findings, and coverage gaps — not from business self-assessment; residual risk is computed, never entered; and every residual risk outside appetite requires a funded mitigation plan with an interim compensating control.

The assessment covers 61 reportable assessment units (business line × region × legal entity), is refreshed annually with a mid-year data refresh, and is refreshed on an event-driven basis on material change. It is approved by the Board.

The Program's connection to the EWRA is not decorative. FCC maintains a **traceability matrix**, tested by Internal Audit, evidencing what changed — in headcount, budget, detection scenarios, thresholds, due diligence calibration, training curriculum, testing scope and risk appetite — as a result of each material EWRA conclusion. A conclusion that changed nothing is treated as a program failure, not as a reassuring result.

8. Program component: customer due diligence and screening

8.1 The principle

The Firm does not do business with a party it does not know. Due diligence is a condition of relationship, not a formality completed afterwards. Where required diligence cannot be completed, the Firm does not open the account, does not process the transaction, and considers whether the circumstances themselves give rise to a reportable suspicion.

8.2 Components

- **Customer identification.** Identify and verify every customer before account opening, to the standard in the Operating Procedures; a hard system block prevents activation without a CIP pass or an approved, time-bound deferral.
- **Beneficial ownership.** Resolve every legal entity to the natural persons who own or control it — 25%, or 10% for High-risk customers, high-risk jurisdictions and private banking — plus a control-prong individual in every case. An entity that cannot be resolved is not onboarded.
- **Risk rating.** Produced solely by a validated model. Upward overrides are free; downward overrides require FCC approval, are 100% QA-reviewed, and are a reported KRI.
- **Enhanced due diligence.** Mandatory for High-risk customers, PEPs, correspondent banks, private banking, and every category on the Restricted Business Schedule. Approved at the authority levels in the Operating Procedures — for senior foreign political figures in private banking, at the Financial Crimes Risk Committee, with annual re-approval.
- **Ongoing review.** 12 / 24 / 36-month cycles by risk band, plus event-driven triggers. A review that does not compare actual activity to expected activity has not been performed.
- **Screening.** Continuous screening of every customer, beneficial owner, controller, signatory and related party against sanctions, PEP, adverse-media and internal watchlists, with four-eyes disposition and evidence-based clearing.

8.3 Prohibited relationships

Shell banks; anonymous and fictitious-name accounts; payable-through arrangements without look-through; entities subject to a Section 311 special measure; bearer-share entities; anonymity-enhancing virtual assets; and any relationship whose beneficial ownership cannot be established. These are hard-blocked in the systems. There is no approval path, and they are not capable of exception — by anyone, at any level.

8.4 The sanctions interface

Sanctions compliance is strict-liability and is governed by the separate Global Sanctions Framework. Nothing in this Program permits a risk-based approach to a sanctions prohibition. The two frameworks are operationally interdependent: information surfaced in AML due diligence, monitoring or investigation that discloses a potential sanctions nexus, an evasion typology or a proliferation-financing indicator must be escalated immediately to the

Global Sanctions Officer; and sanctions screening outcomes indicating potential laundering are escalated into this Program.

9. Program component: detection, investigation and reporting

Stage	How the Program operates it	Key controls
Detection	NG-DETECT runs scenario-based monitoring on a T+1 batch cycle across every in-scope product, entity and channel, with intraday rules for cash and wires. Coverage is reconciled monthly to the Finance product and entity inventory — not to a list FCC maintains itself. Scenarios are mapped to the typologies identified in the EWRA and to the national priorities; a typology with no scenario is an accepted risk requiring BSA/AML Officer sign-off.	AML-TMS-001, 002, 003
Investigation	Three-tier model (L1 triage, L2 investigation, L3 complex case) with defined service levels, a minimum 90-day lookback, mandatory counterparty screening and adverse-media search, and a documentation standard requiring that an independent reader can re-perform the analysis two years later with no other context.	AML-TMS-004, 005, 008
The clock	The **initial detection date** is captured as a mandatory, immutable field at case creation; the statutory 30/60/120-day deadlines are computed from it by the system, not by the investigator, with automated escalation at T-10, T-5 and T-2 days. Internal service levels exist to protect the statutory clock; they never define it.	AML-RPT-002, AML-TMS-006, 008
Reporting decision	The SAR Review Committee, chaired by the Head of Investigations, with FCC Advisory and Legal in attendance. No business representative attends; the revenue of the relationship is not before the Committee. Both FILE and NO-FILE are documented decisions; NO-FILE decisions are 10% QA-sampled and audited. The BSA/AML Officer may direct a filing over the Committee; no one may direct the BSA/AML Officer not to file.	AML-RPT-001, 003
Filing and confidentiality	Filed via FinCEN BSA E-Filing; BSA Identifier reconciled within 5 business days. SAR data is access-controlled, logged, recertified quarterly, and DLP-blocked from shared drives and external email. Tipping off is treated as a potential criminal offence and is escalated immediately to the BSA/AML Officer and Legal.	AML-RPT-004, 005, AML-GOV-006
Other reporting	CTRs (systemic aggregation, 15-day filing, centrally administered exemptions); 314(a) (14-day response, strict confidentiality); 314(b) (FCC only, registration verified, every exchange logged); blocked-property reports (10 business days, via Sanctions).	AML-RPT-006, 007, 008

The Program's single most examined date

In any BSA examination, the initial detection date is tested before almost anything else, because it is the date from which every statutory deadline runs and it is the date most easily — and most quietly — recorded late. Northgate makes it a mandatory, immutable, system-captured field, computes deadlines from it automatically, and logs every attempted change with an approver. This is a deliberate design choice: it removes the possibility of an individual under backlog pressure buying themselves time by recording a later date, and it means the Firm can evidence timeliness rather than assert it.

10. Program component: training, testing and assurance

10.1 Training

- Mandatory AML training on joining and at least annually thereafter for every director, officer, employee and relevant contingent worker. Completion is system-tracked; non-completion escalates to the manager and

suspends system access at day 30.

- Training is risk-based and role-specific. The curriculum is built each year **from the EWRA conclusions and the national priorities** — not from last year's deck. Staff in correspondent banking, private banking, trade finance, payments, onboarding and FCC receive deeper, function-specific content using real typologies and the Firm's own cases.
- Comprehension is assessed with an enforced pass mark. Attendance is not training.
- The Board and its committees receive training sufficient to enable informed oversight and effective challenge — including on what the Program cannot do.

10.2 The three lines and the assurance map

The first line owns and manages the risk it creates. The second line — FCC — owns the framework, the standards, the challenge, the reporting decision and the right to decline and exit. The third line — Internal Audit — provides independent assurance over the whole Program, **including over the second line itself**, and reports directly to the Audit Committee. Internal Audit does not design, own or operate any AML control. The full assurance map, showing which line tests which control domain and at what frequency, is at Appendix B.

10.3 Independent testing

- The AML Program is in permanent Internal Audit scope. Correspondent banking, transaction monitoring and regulatory reporting are audited at least annually. The audit plan is risk-ranked against the EWRA output, and a divergence between the two must be explained to the Audit Committee.
- Where Internal Audit lacks the specialist expertise — for example, in model validation or in a novel product — qualified external parties are engaged, and their independence is assessed before engagement.
- Testing addresses **design** and **operating** effectiveness as separate questions, and requires re-performance from source data. Inspecting the operator's own conclusion and agreeing with it is not testing, and any finding rated on that basis is rejected.
- Findings are tracked to closure with independent validation. A pattern of extension requests is itself reported to the Audit Committee. Businesses must not obstruct, restrict or negotiate the substance of a finding.

11. Program component: technology, data and models

System	Purpose	Governance
NG-KYC	Onboarding workflow, CIP, beneficial ownership, KYC profile, risk rating, periodic review.	Rating model validated under the Model Risk Management Policy; no manual rating path exists.
NG-SCREEN	Sanctions, PEP, adverse-media and internal watchlist screening, at onboarding, on list update, and continuously.	OFAC lists loaded within 4 hours of publication; all others within 24. Quarterly fuzzy-match tuning with above-the-line and below-the-line testing.
NG-DETECT	Scenario-based transaction monitoring across all products, entities and channels.	Coverage reconciled monthly to the Finance inventory. Annual threshold tuning with ATL/BTL testing and a mandatory detection-impact assessment. Independent model validation.
NG-CASE	Alert triage, investigation, case management, SAR decisioning workflow.	Immutable initial-detection date; append-only case records; mandatory-field enforcement before closure.

System	Purpose	Governance
NG-FILE	Regulatory reporting and the BSA E-Filing interface.	Automated deadline computation and escalation; BSA Identifier reconciliation.
NG-GRC	The RCM, issue management, testing results, attestations, the risk assessment.	The single system of record. Shadow control inventories and local spreadsheets are prohibited.

11.1 Data

Detection is only as good as the data it sees. The Program treats data quality as a control domain in its own right, tested across five dimensions — completeness, accuracy, timeliness, coverage and lineage — with daily source-to-target reconciliation, quarterly critical-data-element tracing, and an annual coverage attestation by every business head. A system that is not connected to monitoring is not a data-quality issue; it is a population of transactions that no one is watching, and it is treated as a Critical failure.

11.2 Artificial intelligence and automation

AI and machine-learning techniques may support the Program where they are explainable, validated, monitored for bias and drift, and subject to human review of consequential outcomes. **No automated system may make a final decision to file or not to file a suspicious activity report, or to onboard or exit a client, without qualified human review.** Efficiency gains from automation are reinvested in depth of investigation before they are taken as headcount reductions; where they are taken as headcount reductions, the BSA/AML Officer must state to the Board that the Program remains adequately resourced, in writing.

Prohibited technology practices

Raising a monitoring threshold because alert volume exceeds team capacity. Disabling a scenario to clear a backlog. Excluding a customer, product or corridor from monitoring by exception rather than by design. Presenting a false-positive reduction as a tuning outcome with no below-the-line evidence that nothing true was suppressed. Each of these converts an operational problem into a detection failure, and each has featured in public enforcement actions against other institutions.

12. Resourcing model and budget governance

Under-resourcing is the mechanism by which most AML programs fail. It rarely presents as a decision to under-resource; it presents as a backlog, then as a lowered threshold, then as a missed filing. The Program therefore makes resourcing a governed, evidenced and Board-visible matter.

- The BSA/AML Officer determines the resources, staffing, expertise, data and technology the Program requires — informed by, and traceable to, the EWRA.
- The BSA/AML Officer reports annually to the Board on whether those resources are, in fact, adequate. **Any material shortfall must be reported to the Board in writing at the time it arises**, not deferred to the annual cycle.
- Financial-crime headcount and budget are ring-fenced within the Compliance budget and cannot be reallocated to another function without BSA/AML Officer consent and Risk Committee notification.
- Capacity is monitored as a KRI: FTE per 1,000 alerts; backlog against SLA; vacancy rate; attrition; and average investigator tenure. A capacity KRI in breach is reported to the Financial Crimes Risk Committee with a

recovery plan, and a recovery plan that relies on raising thresholds is rejected on its face.

- The remuneration, performance assessment, promotion and tenure of the BSA/AML Officer and of FCC staff must not be influenced, directly or indirectly, by the commercial outcomes of decisions properly taken under the Program.

13. Global applicability, local addenda and conflicts of law

- **The higher standard governs.** This Program is the minimum standard worldwide. Where local law or supervisory expectation is stricter, the stricter local requirement applies in that jurisdiction. Where local requirements are less strict, this Program applies. Local addenda may raise the standard; they may never lower it, and every addendum is reviewed and approved by FCC and recorded in the policy inventory.
- **Group-wide information sharing.** Financial-crime information is shared within the group for AML purposes to the fullest extent permitted by applicable law and data-protection requirements. This is what allows the Firm to see a customer exited in one region attempting to onboard in another.
- **Conflicts of law.** Where compliance with this Program would require the Firm to breach local law — for example, where secrecy, blocking, data-protection or data-localisation law prohibits the collection, retention or transfer of information the Program requires — the conflict is escalated immediately to FCC and Legal. It must never be resolved unilaterally, locally, or informally.
- FCC and Legal assess the conflict, seek supervisory guidance where appropriate, and determine the Firm's position. **Where the conflict cannot be resolved in a way that allows the Firm to manage the risk to an acceptable standard, the Firm restricts or exits the affected activity.** The Firm does not maintain a business it cannot control. All unresolved conflicts are reported to the Risk Committee of the Board.

14. Program effectiveness: how the Firm measures whether this works

The AML Act of 2020 requires programs to be effective, not merely present. Effectiveness is not self-evident from the existence of policies, the volume of SARs filed, or the absence of an enforcement action. The Firm measures it deliberately, on four axes, and reports the result to the Board annually alongside the EWRA.

Axis	The question	How it is evidenced
Coverage	Is the Firm looking everywhere it should be looking?	Monitoring and screening coverage reconciled to the Finance product and entity inventory; the gap register with expiry dates; typology-to-scenario mapping; data completeness reconciliations.
Detection quality	When something is wrong, does the Firm find it?	Below-the-line testing on screening and monitoring thresholds; outcomes analysis — for every SAR filed, was it generated by a scenario, by an employee, or by a law-enforcement enquiry? A rising proportion sourced from law-enforcement enquiry is a detection failure, however good the response was.
Response quality	When the Firm finds something, does it act properly and on time?	Filing timeliness against the initial detection date (target: zero late); QA error rates by grade; SAR narrative quality scores; alert ageing; overdue periodic reviews; law-enforcement feedback on filing usefulness where available.
Institutional health	Would this Firm find out if it had a problem?	Self-identification rate — what proportion of issues were found by the Firm itself rather than by audit or a regulator? Escalation and whistleblowing volumes. Investigator tenure and attrition. Downward override rates. Whether any business has attempted to influence a compliance decision, and what happened to them.

The uncomfortable metric

Self-identification rate is the metric that most distinguishes a healthy program from a compliant-looking one. A firm that finds its own problems has a functioning control environment and a culture in which people can say so. A firm whose issues are almost all found by Internal Audit or by the examiner has neither — regardless of how many controls are in its RCM. Northgate reports this figure to the Board every quarter, unrounded, with the trend.

15. Regulatory engagement, examinations and issue remediation

- All contact with regulators and law-enforcement authorities on financial-crime matters is coordinated through FCC and Legal. No individual responds unilaterally to a regulatory or law-enforcement request, and no individual may obstruct, delay or influence the Firm's response.
- The Firm engages with its supervisors **candidly and proactively**. Where the Firm identifies a material control failure, a coverage gap, or a potential pattern of missed filings, it self-reports — it does not wait to be found. Self-reporting is a matter of policy and of self-interest: the difference in outcome between a self-reported issue and a discovered one is the difference between a remediation plan and a consent order.
- Examination and audit findings are tracked in NG-GRC with named individual owners, root cause, target dates and independent validation of closure. Extensions are governed and reported; a second extension escalates automatically to the Financial Crimes Risk Committee.
- **Where an issue reveals that a control was ineffective for a period, a lookback is mandatory.** The Firm must establish what activity occurred while the control was not working, and whether any of it required a filing. Retrospective filings are made as soon as suspicion is formed, not at the conclusion of the exercise. Fixing a control forward without a lookback leaves the original suspicion unreported — which is the failure, not the broken control.

16. Mergers, acquisitions and new business

- **New products, services, channels and markets.** No new product, service, channel, market or technology — and no material change to an existing one — may be approved or launched without a documented financial-crime risk assessment and the written concurrence of FCC, which includes an assessment of whether the activity can be monitored and screened on day one. FCC may withhold concurrence, and the product does not proceed without it.
- **Acquisitions and portfolio purchases.** Financial-crime due diligence is mandatory in pre-acquisition diligence: the target's customer base, its historic due diligence, its unresolved suspicious activity, its monitoring coverage and its regulatory history. A funded, time-bound remediation plan must be approved **before close** where gaps are identified.
- **Inherited deficiencies become the Firm's deficiencies on day one.** There is no grace period in law. An acquired book with inadequate KYC is, from completion, a Northgate book with inadequate KYC, and the Firm will be examined on that basis. Integration plans that defer AML remediation behind commercial integration are rejected.
- **Integration.** The acquired entity is brought into this Program, the EWRA, the RCM and the monitoring estate on a defined and Board-visible timeline. Until it is, its risk is assessed and reported separately, and any monitoring gap is treated as a Critical issue with an interim compensating control.

17. Annual program calendar and Board reporting

Period	Program activity
Q1 (Jan–Mar)	Prior-year program effectiveness assessment. Board reapproval of the Policy and this Program. Annual control attestation by every control owner. Training curriculum launched. Independent testing plan approved by the Audit Committee.
Q2 (Apr–Jun)	Country Risk List annual review. Restricted Business Schedule review. Model validation cycle. Mid-year EWRA data refresh. Threshold tuning (ATL/BTL) for monitoring and screening.
Q3 (Jul–Sep)	EWRA fieldwork: data extraction, business submissions, independent FCC scoring, challenge sessions, action-plan agreement. Draft EWRA to the Financial Crimes Risk Committee by 30 September.
Q4 (Oct–Dec)	Model Risk validation of the EWRA methodology. Internal Audit review of the EWRA process. EWRA to the Board Risk Committee and the Board. Cascade into next year’s budget, headcount, testing plan, audit plan, training curriculum and tuning schedule. Traceability matrix updated.
Continuous	Financial Crimes Risk Committee (monthly). SAR Review Committee (twice weekly). KRI dashboard (monthly). Board Risk Committee reporting (bi-monthly). Issue and finding tracking. Regulatory engagement.

Appendix A — Legal entity and regulator matrix

Legal entity	Jurisdiction	Principal regulator(s)	Local AML officer
Northgate Financial Group, Inc. (holding company)	United States	Federal Reserve	BSA/AML Officer (group)
Northgate Bank, N.A.	United States	OCC; FinCEN; FDIC (deposit insurance)	BSA/AML Officer
Northgate Securities LLC	United States	SEC; FINRA (Rule 3310); FinCEN (31 CFR § 1023.210)	Designated AML Compliance Officer
Northgate Trust Company, N.A.	United States	OCC	Entity AML Officer
Northgate Bank, London Branch	United Kingdom	PRA; FCA (MLRs 2017)	MLRO
Northgate Bank Frankfurt GmbH	Germany	BaFin; ECB (via SSM)	Geldwäschebeauftragter
Northgate Bank, Singapore Branch	Singapore	MAS	Head of Compliance / MLRO
Northgate Bank, Hong Kong Branch	Hong Kong SAR	HKMA; SFC (for regulated activities)	MLRO
Northgate Bank (DIFC) Limited	UAE — DIFC	DFSA	MLRO
Northgate Asset Management Ltd	United Kingdom	FCA	MLRO
Northgate Digital Assets LLC	United States	FinCEN (MSB registration); state regulators	Designated AML Officer
Northgate Bank Toronto Branch	Canada	OSFI; FINTRAC	Chief Anti-Money Laundering Officer
Northgate Bank São Paulo	Brazil	Banco Central do Brasil; COAF	Diretor de Compliance
Northgate Bank Sydney Branch	Australia	APRA; AUSTRAC	AML/CTF Compliance Officer

Every local AML officer reports functionally to the BSA/AML Officer and holds equivalent local independence, authority, access, resourcing and protection. A local officer may not be removed without the BSA/AML Officer's concurrence, and any removal is reported to the relevant local regulator.

Appendix B — Assurance map

Control domain	1LOD self-testing	2LOD (CTM)	3LOD (Internal Audit)	External
Customer identification and beneficial ownership	Quarterly	Annual, all Key Controls	Annual	—
Risk rating and EDD	Quarterly	Annual + thematic on overrides	Annual	Model validation
Screening (PEP / adverse media)	Quarterly	Annual + quarterly ATL/BTL	Annual	Independent tuning review, biennial
Sanctions screening and blocking	Monthly	Quarterly	Annual	Independent testing, annual
Transaction monitoring coverage and scenarios	Monthly	Annual + tuning validation	Annual	Model validation, annual

Control domain	1LOD self-testing	2LOD (CTM)	3LOD (Internal Audit)	External
Alert handling and investigation	Continuous QA	Annual + thematic	Annual	—
SAR decisioning, narrative and filing timeliness	Continuous QA (10% of no-file decisions)	Annual	**Annual, mandatory**	—
CTR and 314(a)	Monthly	Annual	Annual	—
Correspondent banking	Monthly	Annual	**Annual, mandatory**	Periodic external review
Recordkeeping and retention	Annual	Biennial	Risk-based	—
Data quality and system coverage	Daily / quarterly	Quarterly CDE tracing	Annual	—
Training	Annual	Annual	Risk-based	—
Governance, EWRA and risk appetite	—	Methodology validation (Model Risk)	**Annual, mandatory**	Regulatory examination

Appendix C — Board reporting pack: mandatory contents

The quarterly financial-crime pack to the Risk Committee, and the annual pack to the Board, must contain each of the following. Items may not be omitted because they are unfavourable, and adverse trends must be presented as adverse.

- The BSA/AML Officer’s own opinion on program effectiveness, stated plainly, in the Officer’s own words, at the front of the pack — not buried in an appendix and not edited by any business.
- Residual risk position against appetite, by assessment unit, with every High and Very High cell explained in narrative.
- Every risk acceptance in force, its expiry date, and whether it has been re-approved on its merits.
- Filing timeliness: SARs, CTRs, 314(a) responses and blocked-property reports — with the number filed late stated as an absolute number, not as a percentage.
- Alert and case backlog and ageing, against the statutory clock, not against internal service levels.
- Monitoring and screening coverage gaps, with the affected population and the compensating control.
- Open issues and findings by severity and age; overdue items by name; extension requests and their pattern.
- The self-identification rate and its trend (§ 14).
- KRI dashboard with every amber and red metric explained, and any metric whose threshold was changed during the period disclosed as such.
- Resourcing: FTE against plan, vacancy rate, attrition, capacity KRIs — and the BSA/AML Officer’s written statement of whether resources remain adequate.
- Any instance in which a business attempted to influence, delay or override a compliance decision, and what was done about it.
- Material regulatory and law-enforcement developments, examinations in progress, and any self-report made to a regulator.

Approval

This Enterprise-Wide Global AML Program was approved by the Board of Directors of Northgate Financial Group, Inc. on 12 March 2026, on the recommendation of the Risk Committee and the Audit Committee, and the approval was recorded in the minutes of that meeting. The Program is reapproved by the Board at least annually.

_____

Chair of the Board of Directors

_____

Chief Executive Officer

_____

Chief Compliance Officer

_____

Global Head of Financial Crimes Compliance
(designated BSA/AML Officer)

— End of Program —