Global Anti-Money Laundering Policy

This Policy establishes the minimum standards that govern how Northgate Financial Group, Inc. and each of its subsidiaries, branches and affiliates worldwide identify, assess, mitigate, monitor and report money laundering and terrorist financing risk. It is a statement of mandatory principle and accountability. It does not prescribe operating procedures, system configurations or control designs; those are issued separately under the authority of this Policy.

Document control	Detail
Document title	Global Anti-Money Laundering Policy
Document classification	Level 1 — Firmwide Policy (Board-Approved)
Version	9.0 (supersedes Version 8.3, effective 1 April 2025)
Policy owner	Global Head of Financial Crimes Compliance; designated BSA/AML Officer under 31 CFR § 1020.210
Accountable executive	Chief Compliance Officer
Approved by	Board of Directors, on the recommendation of the Risk Committee and the Audit Committee
Date approved	12 March 2026
Effective date	1 April 2026
Review cycle	Annual; and upon material change in law, regulation, business model, risk profile or supervisory expectation
Next scheduled review	31 March 2027
Applies to	All legal entities, business lines, branches, representative offices and majority-owned subsidiaries of Northgate Financial Group, Inc., globally
Related Level 1 policies	Global Sanctions Policy; Anti-Bribery and Corruption Policy; Anti-Fraud Policy; Client Onboarding and Due Diligence Policy; Code of Conduct; Enterprise Risk Management Framework

Illustrative training specimen. “Northgate Financial Group, Inc.” is a fictional institution created for instructional use; the document is modelled on the structure and register of a US Category I bank holding company AML policy and is not the policy of any real firm.

Table of Contents

How to read this document

This is a Level 1 Policy. It states **what must be true** at Northgate and **who is accountable** for making it true. It deliberately does not state **how** any requirement is executed. Standards, procedures, control designs, system rules, thresholds, escalation matrices and desk-level instructions are set out in Level 2 Standards and Level 3 Procedures issued under the authority of, and subordinate to, this Policy. Where a Level 2 or Level 3 document conflicts with this Policy, this Policy prevails and the conflict must be reported to the Policy owner.

1. Purpose and Policy Statement

Northgate Financial Group, Inc. and its subsidiaries (together, "Northgate" or the "Firm") are entrusted with access to the United States and international financial systems. That access carries an obligation to prevent the Firm from being used, knowingly or unknowingly, to launder the proceeds of crime, to finance terrorism, or to move funds connected to corruption, human trafficking, narcotics, fraud, proliferation or any other unlawful purpose.

The purpose of this Policy is to establish a single, mandatory, firmwide standard for the prevention, detection and reporting of money laundering and terrorist financing ("ML/TF"), and to make explicit the governance, accountability and escalation expectations that support it.

> **Policy statement of the Board of Directors**
>
> Northgate does not tolerate money laundering, terrorist financing, or the facilitation of either. The Firm will not accept, retain or process business where the ML/TF risk cannot be understood, evidenced and managed within the Firm's stated risk appetite — regardless of the revenue, client relationship, strategic priority or commercial pressure involved. Compliance with this Policy is a condition of employment and of doing business with the Firm. No employee has the authority to waive it, and no business objective may be pursued at its expense.

1.1 Objectives

- Protect the Firm, its clients, its shareholders and the integrity of the financial system from abuse by illicit actors.
- Ensure that the Firm meets, at a minimum, all applicable AML/CFT legal and regulatory obligations in every jurisdiction in which it operates.
- Establish clear, unambiguous individual accountability for ML/TF risk, from the Board to the front line.
- Ensure that ML/TF risk is identified and assessed before it is assumed, and is managed on a risk-sensitive basis thereafter.
- Ensure that suspicious activity is escalated, investigated and reported to the relevant authorities promptly, completely and in confidence.
- Embed a culture in which raising a financial-crime concern is expected, protected and recognised, and in which no individual is disadvantaged for doing so.

2. Scope and Application

This Policy applies globally and without exception to:

- every legal entity in which Northgate Financial Group, Inc. holds a direct or indirect majority interest, or over which it exercises control, including all US and non-US bank and non-bank subsidiaries, branches, agencies and representative offices;
- every business, product, service, channel, and geography through which the Firm operates, including consumer and community banking, commercial banking, corporate and investment banking, markets, private banking and wealth management, asset management, payments, custody, correspondent banking and digital-asset activities;
- every director, officer, employee, secondee, intern and contingent worker of the Firm, irrespective of location, seniority, function or reporting line; and

- every agent, introducer, distributor, service provider and other third party acting for or on behalf of the Firm, to the extent set out in Section 16.

Non-controlled joint ventures and minority investments are not directly bound by this Policy. Where the Firm holds such an interest, the responsible business must nonetheless assess the ML/TF risk arising from the investment, and Financial Crimes Compliance ("FCC") must be satisfied that the Firm's own exposure is acceptable and that the Firm can exit if it is not.

2.1 Standard of application — the higher standard governs

This Policy sets the **minimum** standard for the Firm worldwide. Where local law, regulation or supervisory expectation in a jurisdiction imposes a **stricter** requirement than this Policy, the stricter local requirement applies in that jurisdiction. Where local requirements are **less strict**, this Policy applies. Local addenda may raise the standard; they may never lower it. Every local addendum must be reviewed and approved by FCC and recorded in the Firm's policy inventory.

Where the Firm cannot apply this Policy in a jurisdiction because local law prohibits it, Section 23 (Conflicts of Law) applies.

2.2 Relationship to other policies

The Firm maintains separate Level 1 policies for economic sanctions, anti-bribery and corruption, anti-fraud, anti-tax-evasion facilitation, and client onboarding. Those policies are complementary to, and read together with, this Policy. Where an activity engages more than one policy — for example, a payment involving both a sanctions nexus and an unexplained third-party flow — all applicable policies apply concurrently and the most restrictive outcome governs.

Applies to	Requirement in scope
All employees and contingent workers	Complete assigned AML training; know your obligations; escalate anything that does not make commercial sense; never tip off a client.
Client-facing and revenue-generating staff	Own the ML/TF risk of the relationships you introduce and maintain; provide complete and accurate client information; do not proceed where due diligence is incomplete.
Operations, technology and service functions	Execute controls as designed; report control failures; preserve records; protect the confidentiality of suspicious activity reporting.
Managers and business heads	Ensure the business does not accept risk beyond the approved appetite; ensure adequate resourcing; act on FCC findings; do not incentivise behaviour inconsistent with this Policy.
Directors and senior executives	Set the tone; oversee the program; ensure the BSA/AML Officer has the independence, standing and resources required by Section 7.

3. Risk Appetite and Prohibited Activity

The Board sets the Firm's financial-crime risk appetite as part of the Enterprise Risk Appetite Statement. The Firm's appetite for ML/TF risk is **low**. The Firm accepts that it cannot reduce ML/TF risk to zero while providing financial services; it does not accept relationships or activity whose risk it cannot identify, evidence, price and control.

Risk appetite is expressed and monitored through qualitative statements and quantitative measures approved by the Risk Committee and cascaded to each business. Breaches of appetite are reported to the Risk Committee and, where material, to the Board.

3.1 Prohibited relationships and activity

The following are prohibited firmwide. They are not subject to business-level risk acceptance, and they may not be approved by exception under Section 22:

- **Shell banks.** Establishing, maintaining, administering or managing a correspondent account for a foreign shell bank, or for any foreign bank that permits use of its account by a foreign shell bank.
- **Anonymous and fictitious-name accounts.** Opening or maintaining any account in an anonymous, numbered-only or knowingly fictitious name, or any account where the customer and beneficial owner cannot be identified and verified.
- **Payable-through arrangements without transparency.** Permitting a foreign financial institution's customers direct transactional access to a Northgate account where those underlying customers are not identified and subject to due diligence.
- **Entities subject to special measures.** Any relationship or transaction prohibited by a special measure imposed under Section 311 of the USA PATRIOT Act, or by any equivalent measure of another competent authority.
- **Bearer-share entities.** Onboarding or maintaining a legal entity whose ownership can be transferred by bearer instrument such that beneficial ownership cannot be reliably determined and kept current.
- **Anonymity-enhancing digital assets.** Transacting in, custodying or providing services in respect of virtual assets designed to defeat traceability, or dealing with virtual-asset service providers that lack an AML program the Firm can evidence.
- **Facilitation.** Knowingly structuring, restructuring, layering or documenting any transaction, entity or account for the purpose of concealing beneficial ownership, source of funds, source of wealth, purpose, or the involvement of a sanctioned or criminal party — or of evading a reporting or recordkeeping obligation.
- **Concealment from regulators or auditors.** Withholding, altering, backdating or destroying information sought by a regulator, law-enforcement authority, Internal Audit or FCC.

> **The single most important sentence in this Policy**
>
> If a transaction, client, structure or instruction does not make commercial sense to you, or you cannot explain it to someone outside the deal, you must escalate it. You are not required to be certain, to prove anything, or to be right. You are required to raise it. Failing to raise it is a disciplinary matter; raising it in good faith never is.

3.2 Restricted activity

Certain business is permitted only within defined limits and with defined approvals. Restricted activity includes, without limitation, business involving jurisdictions designated by the Firm as high risk; foreign correspondent banking; private banking for senior foreign political figures; cash-intensive businesses; money services businesses; virtual-asset service providers; embassies and foreign missions; and clients whose structures involve nominee arrangements or multi-layered offshore vehicles. The Firm maintains a Restricted Business Schedule, owned by FCC and approved by the Financial Crimes Risk Committee, that lists such activity and the approval authority required in each case. No business may be accepted outside the approvals set out in that Schedule.

3.3 The right to decline and to exit

FCC has the unconditional authority to decline the onboarding of a prospective client, to decline a transaction, to impose conditions on a relationship, and to require the exit of an existing relationship, on financial-crime grounds. That authority may not be overridden by any business or by any individual, however senior. A business may escalate a decision to the Financial Crimes Risk Committee; it may not disregard it, delay it, or seek to relitigate it through a different channel. Exit decisions are executed in a manner that avoids tipping off and preserves the Firm's reporting obligations.

4. Legal and Regulatory Framework

This Policy is designed to enable compliance with, and is informed by, the following principal authorities. This list is illustrative, not exhaustive; the absence of an authority from this list does not relieve the Firm of any obligation.

Source	Principal obligations reflected in this Policy
Bank Secrecy Act (31 U.S.C. 5311 et seq.) and its implementing regulations at 31 CFR Chapter X	Maintain an effective, risk-based AML program; report currency transactions and suspicious activity; keep prescribed records; comply with funds-transfer recordkeeping and transmittal requirements.
USA PATRIOT Act (2001)	Customer identification (Sec. 326); enhanced due diligence for foreign correspondent and private banking accounts (Sec. 312); prohibition on foreign shell bank correspondents (Sec. 313); information sharing with government and between financial institutions (Sec. 314(a) and 314(b)); special measures (Sec. 311); foreign bank records and summons (Sec. 319).
Anti-Money Laundering Act of 2020, including the Corporate Transparency Act	Effectiveness and risk-based prioritisation of the AML program; national AML/CFT priorities; beneficial-ownership transparency; strengthened whistleblower protection; expanded penalties and the presumption that compliance is a firmwide obligation.
FinCEN CDD Rule (31 CFR § 1010.230) and 31 CFR § 1020.210	Identify and verify beneficial owners of legal entity customers; understand the nature and purpose of customer relationships; conduct ongoing monitoring and update customer information on a risk basis; maintain the five pillars of an AML program.
Regulations and supervisory expectations of the OCC, the Federal Reserve, the FDIC, the SEC and FINRA, as applicable to the relevant Northgate entity	Program adequacy; board and senior-management oversight; independent testing; qualified and independent BSA/AML Officer; remediation of supervisory findings.
FFIEC BSA/AML Examination Manual	Supervisory benchmark against which the design and effectiveness of the Firm's program is assessed.
Office of Foreign Assets Control (31 CFR Chapter V)	Sanctions compliance; blocking and rejecting; reporting. Governed principally by the Global Sanctions Policy (see Section 14).
Financial Action Task Force Recommendations; EU AML Directives and the EU AML Regulation; UK Money Laundering Regulations; and other applicable local regimes	Minimum international and local standards applied to the Firm's non-US operations.

5. Governance and Oversight

The Firm governs ML/TF risk through a defined structure of Board and management bodies with documented mandates, quorum requirements, escalation paths and minuted decisions. No body may sub-delegate accountability for a matter reserved to it under this Policy.

5.1 Board of Directors

The Board is ultimately accountable for the Firm's AML program. The Board:

- approves this Policy and any material amendment to it, at least annually;
- approves the Firm's financial-crime risk appetite;
- appoints and, where necessary, removes the BSA/AML Officer, and satisfies itself that the individual is qualified, independent, senior and adequately resourced;
- receives and considers the annual Enterprise-Wide ML/TF Risk Assessment, the annual AML Program effectiveness report, and the results of independent testing;
- oversees the timely remediation of material regulatory findings, internal audit findings and self-identified issues; and
- sets the tone from the top and holds executive management accountable for the culture described in Section 20.

The Board discharges these responsibilities directly and through its Risk Committee and Audit Committee, but it does not thereby transfer accountability.

5.2 Risk Committee of the Board

The Risk Committee oversees financial-crime risk as a component of non-financial risk. It reviews the enterprise risk assessment, monitors risk-appetite metrics and breaches, reviews significant regulatory developments and enforcement matters, and receives a standing report from the BSA/AML Officer at each scheduled meeting. It escalates to the full Board any matter that is material to the Firm's risk profile, capital, licences or reputation.

5.3 Audit Committee of the Board

The Audit Committee oversees the independence, scope, methodology and adequacy of independent testing of the AML program, and monitors the closure of audit findings. The Chief Audit Executive has a direct, unfiltered reporting line to the Audit Committee.

5.4 Financial Crimes Risk Committee (management)

The Financial Crimes Risk Committee is the senior executive forum for financial-crime risk. Chaired by the BSA/AML Officer and comprising the heads of each business, Operations, Technology, Legal, Risk and Internal Audit (as observer), it:

- reviews the aggregate ML/TF risk profile of the Firm and of each business;
- acts as the escalation and decision forum for the highest-risk relationships, including those requiring senior-management approval under Section 11;
- approves the Restricted Business Schedule and the Firm's country-risk ratings;
- reviews thematic findings, systemic control weaknesses and remediation progress; and
- decides contested exit recommendations, subject always to Section 3.3.

Decisions of the Committee are minuted, including dissent. Where the Committee approves a relationship over the objection of FCC, the matter is reported to the Risk Committee of the Board at its next meeting.

5.5 Management information

The Board and its committees must receive management information sufficient to allow them to challenge, not merely to note. Reporting must be accurate, timely, complete, and presented so that adverse trends, thresholds breached, and matters requiring attention are visible without inference. FCC owns the integrity of financial-crime management information; no business may filter, soften or delay it.

6. Roles, Responsibilities and the Three Lines of Defense

The Firm operates a three-lines-of-defense model. Accountability for ML/TF risk sits first and foremost with the business that generates it. Compliance does not own the risk; it owns the framework, the standards and the independent challenge.

Line	Who	Accountable for
First line	All business lines and revenue-generating functions; and the operational functions that support them	Owning and managing the ML/TF risk they create. Knowing their clients. Providing complete and accurate client and transaction information. Performing the controls assigned to them. Escalating unusual activity. Not accepting business outside appetite. Ensuring their incentive and performance arrangements never reward the circumvention of this Policy.
Second line	Financial Crimes Compliance, under the BSA/AML Officer; supported by Compliance, Legal and Operational Risk	Setting the framework, standards and risk appetite methodology. Owning the enterprise risk assessment. Designing and calibrating monitoring and screening standards. Deciding suspicious activity reporting. Providing independent challenge to the first line. Exercising the right to decline and to exit. Reporting to the Board.
Third line	Internal Audit	Providing independent, objective assurance over the design and operating effectiveness of the AML program, including the work of the second line. Reporting directly to the Audit Committee. Internal Audit does not design, own or operate any AML control.

6.1 Individual accountability

Every employee is personally accountable for compliance with this Policy. Accountability is not discharged by asserting that another function “should have caught it,” by pointing to a system that did not alert, or by relying on the seniority of the person who gave the instruction. An instruction to breach this Policy is void, must be refused, and must be escalated.

Senior executives with designated responsibilities under applicable regulatory regimes (including, where relevant, the UK Senior Managers and Certification Regime and equivalent regimes elsewhere) hold documented, individual responsibility for the financial-crime controls within their remit, recorded in statements of responsibility maintained by Human Resources and Legal.

7. Independence, Authority and Resourcing of the BSA/AML Officer

The Board appoints a qualified individual as the Firm's designated BSA/AML Officer, who serves as Global Head of Financial Crimes Compliance. The Board affirms the following as conditions of the role, and will not permit them to be diluted:

- **Independence.** The BSA/AML Officer does not report to any revenue-generating business and has no revenue, sales or profit-and-loss responsibility. The role reports to the Chief Compliance Officer with a direct, unrestricted reporting line to the Risk Committee of the Board.
- **Access.** The BSA/AML Officer has unrestricted access to all Firm records, systems, data, personnel, premises and third-party arrangements necessary to discharge the role, and to the Board and its committees without the presence of executive management.
- **Authority.** The BSA/AML Officer has the authority to decline business, to require exits, to impose conditions and restrictions, to suspend activity pending investigation, and to file suspicious activity reports — in each case without the consent of, and without consultation with, any business.
- **Resourcing.** The BSA/AML Officer determines the resources, staffing, expertise, data and technology the program requires, and 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.
- **Protection.** The remuneration, performance assessment, promotion and continued 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 this Policy.
- **Removal.** The BSA/AML Officer may be removed only by resolution of the Board, and any such removal, together with the reasons for it, will be reported to the Firm's primary federal regulators.

The BSA/AML Officer may delegate execution but not accountability. Local Money Laundering Reporting Officers appointed in non-US jurisdictions report functionally to the BSA/AML Officer and hold equivalent local independence and authority.

8. The AML Program — Mandatory Pillars

The Firm maintains a written, risk-based AML program, approved by the Board and recorded in the minutes, that satisfies the statutory pillars and is designed to be **effective** in practice and not merely compliant in form. The Board requires that the program be commensurate with the Firm's size, complexity, products, customers and geographies, and that it give priority to the risks that matter most, including the AML/CFT national priorities published by FinCEN.

Pillar	Board requirement
1. Internal controls, policies and procedures	A documented, current and enforced control framework, reasonably designed to prevent, detect and report ML/TF, and to comply with all applicable requirements.
2. Designated compliance officer	A qualified, independent, empowered and adequately resourced BSA/AML Officer, appointed by the Board, with the standing described in Section 7.
3. Ongoing employee training	Role-relevant, risk-based, mandatory training with tracked completion and demonstrable comprehension, as set out in Section 18.
4. Independent testing	Independent, competent, adequately scoped and sufficiently frequent testing of the program, reporting to the Audit Committee, as set out in Section 19.

Pillar	Board requirement
5. Customer due diligence	Risk-based identification and verification of customers and beneficial owners; understanding of the nature and purpose of each relationship; and risk-based ongoing monitoring, as set out in Sections 10 and 11.
Cross-cutting: risk assessment and effectiveness	A documented enterprise-wide risk assessment that drives resource allocation and control calibration, and a periodic assessment of whether the program is achieving its objectives in practice.

9. Enterprise-Wide Money Laundering Risk Assessment

The Firm must know its own risk before it can manage it. FCC owns and performs, at least annually and upon any material change, a documented Enterprise-Wide ML/TF Risk Assessment that:

- identifies and assesses inherent risk across customers, products and services, delivery channels, transactions and geographies;
- evaluates the design and operating effectiveness of the controls applied to that inherent risk;
- derives a residual risk rating for the Firm, for each legal entity and for each business line;
- explicitly incorporates the applicable national AML/CFT priorities and the Firm’s own typologies, alerts, cases, reports filed and adverse events; and
- identifies where residual risk exceeds appetite and what will be done about it, by whom, and by when.

The risk assessment is not an academic exercise. Its conclusions must demonstrably drive the allocation of people, budget and technology; the calibration of due diligence and monitoring; the content of training; and the coverage of independent testing. Where the assessment identifies a risk that the Firm is not equipped to manage, the Firm reduces or exits the risk. It does not accept it by default.

Each business must maintain a business-level risk assessment consistent with the enterprise methodology. Businesses may not adopt their own methodology, rating scale or definitions.

10. Customer Due Diligence and Beneficial Ownership

The Firm will not do business with a party it does not know. Due diligence is a condition of relationship, not a formality to be completed after the fact.

10.1 Minimum principles

- **Identify and verify.** Every customer must be identified and their identity verified using reliable, independent source documents, data or information, before the relationship is established and before transactional access is granted.
- **Look through the structure.** For legal entity customers, the Firm must identify and verify the natural persons who ultimately own or control the entity, and the natural person who exercises significant control over it. An entity whose ultimate beneficial ownership cannot be established to the Firm’s satisfaction must not be onboarded.
- **Understand the relationship.** The Firm must understand and record the nature and intended purpose of each relationship, the expected activity, and, on a risk basis, the source of funds and the source of wealth.

- **Risk-rate every customer.** Every customer must carry a documented ML/TF risk rating that determines the depth of diligence applied and the frequency of review. Ratings must be produced by an approved methodology, not by individual judgement alone.
- **Keep it current.** Customer information must be refreshed on a risk-sensitive basis and whenever a trigger event indicates that the Firm's understanding of the customer may no longer be accurate.
- **No business without diligence.** Where required due diligence cannot be completed, the Firm must not open the account, must not process the transaction, and must consider whether the circumstances give rise to a suspicion that must be reported.

> **Prohibition on retrospective diligence**
>
> It is a breach of this Policy to onboard a client, execute a transaction or extend credit on the understanding that outstanding due diligence will be completed later, unless a formal, time-bound, documented deferral has been granted in advance by FCC at the authority level set in the Restricted Business Schedule. Deferrals are exceptional, are tracked, and are reported to the Financial Crimes Risk Committee. Commercial urgency is not a basis for deferral.

10.2 Accuracy of information

The first line is accountable for the completeness and accuracy of the client information it provides. Knowingly recording inaccurate information, omitting adverse information, or presenting a client's profile in a way designed to secure a lower risk rating is a serious disciplinary matter and may constitute a criminal offence.

11. Higher-Risk Relationships and Activities

Where a relationship presents heightened ML/TF risk, the Firm applies enhanced due diligence, senior-management approval and intensified ongoing scrutiny proportionate to that risk. The categories below are treated as higher risk by default; the list is not exhaustive, and a relationship in no listed category may still be rated high on the facts.

Category	Policy requirement
Foreign correspondent banking	Enhanced due diligence on the respondent, its ownership, its AML program, its supervision, and the markets it serves. The Firm must understand who the respondent's customers are and what activity will flow through the account. Nested and downstream correspondent activity must be identified, understood and either controlled or prohibited. Relationships with respondents in high-risk jurisdictions require approval at the Financial Crimes Risk Committee.
Private banking for senior foreign political figures	Enhanced scrutiny of the source of funds and source of wealth of the individual, their immediate family and close associates, and reasonable steps to detect and report the proceeds of foreign corruption. Senior-management approval is required to establish and to continue the relationship.
Politically exposed persons generally	Risk-based identification of PEPs, their family members and close associates, at onboarding and on an ongoing basis. PEP status is a risk factor, not an automatic bar; it is never a factor to be ignored, and it may never be removed from a record without documented justification.

Category	Policy requirement
High-risk jurisdictions	Country risk ratings are set centrally by FCC and approved by the Financial Crimes Risk Committee, informed by FATF listings, sanctions exposure, corruption indices, narcotics and trafficking exposure, secrecy characteristics and the Firm's own experience. Business in the highest-rated jurisdictions requires elevated approval and is subject to enhanced monitoring.
Cash-intensive businesses; money services businesses; virtual-asset service providers; gaming; precious metals and stones; embassies and foreign missions	Enhanced due diligence, documented approval at the level set in the Restricted Business Schedule, and heightened ongoing monitoring. The Firm does not de-risk entire customer categories reflexively; it assesses each relationship on its individual merits and its ability to control the risk.
Complex, opaque or unexplained structures; nominee arrangements; trusts and foundations with concealed control	The Firm must understand why the structure exists. Where the commercial rationale for opacity cannot be established, the relationship must be declined or exited.
Trade finance and trade-based money laundering exposure	Enhanced scrutiny of parties, goods, routes, pricing and documentation, with particular attention to dual-use and sanctions-relevant goods, price and quantity anomalies, and circular or unnecessary intermediation.
Correspondent, custody and omnibus arrangements where the Firm cannot see the underlying party	Permitted only where the Firm can obtain the information it needs, on request and within a defined period, to identify the underlying party and the purpose of the activity.

11.1 De-risking

The Firm does not terminate or refuse relationships solely on the basis of a customer's category, nationality, religion, or lawful line of business. Exit decisions must be based on the ML/TF risk of the specific relationship, the Firm's ability to manage that risk, and the Firm's appetite — assessed on documented facts, and taken by FCC.

12. Transaction Monitoring and Suspicious Activity Reporting

The Firm monitors customer activity for the purpose of identifying and reporting suspicious activity. Monitoring is risk-based, covers all relevant products, channels and entities, and is subject to governance over its coverage, calibration, tuning and effectiveness. The design, thresholds and scenario logic of monitoring are set out in Level 2 Standards; they are not matters for this Policy.

12.1 Duty to escalate

Every employee has a personal and non-delegable duty to escalate promptly, through the prescribed internal channel, any activity, instruction, client behaviour, structure or circumstance that appears unusual, that lacks an apparent lawful purpose, or that the employee suspects may involve criminal property or terrorist financing. The duty is engaged by suspicion, not by proof. It applies regardless of whether a system generated an alert, and regardless of the seniority of anyone involved.

12.2 Reporting decision

The decision to file a Suspicious Activity Report — or the equivalent report in any other jurisdiction — rests exclusively with FCC and, ultimately, with the BSA/AML Officer or the relevant local Money Laundering

Reporting Officer. That decision:

- is made independently, on the facts, and free from commercial or relationship considerations;
- may not be influenced, delayed, second-guessed or vetoed by any business, however senior;
- is documented, whether the outcome is to report or not to report; and
- is made and filed within the timeframes required by applicable law.

The filing of a report does not, of itself, require the Firm to terminate a relationship, nor does it permit the Firm to continue one it should exit. Those are separate decisions, taken by FCC on the facts.

> **Confidentiality and tipping off**
>
> The existence, contents, and the fact of consideration of a suspicious activity report — and any information that would reveal them — are strictly confidential. No employee may disclose them to the customer, to any person outside the Firm, or to any person inside the Firm without a need to know. Disclosure may be a federal criminal offence. If you are asked about a report by a customer, a third party, or anyone other than FCC, you must not confirm or deny its existence, and you must notify FCC immediately.

12.3 Cooperation with authorities

The Firm cooperates fully, promptly and in good faith with competent law-enforcement, regulatory and financial-intelligence authorities. All contact with such authorities in relation to financial crime is coordinated through FCC and Legal. No employee may respond unilaterally to a law-enforcement request, and no employee may obstruct, delay or influence the Firm’s response.

13. Regulatory Reporting, Recordkeeping and Information Sharing

The Firm files all reports required by law — including currency transaction reports, suspicious activity reports, and reports of foreign financial accounts and monetary instruments — accurately, completely and within the prescribed deadlines. The Firm does not structure, split, sequence, characterise or record any transaction so as to avoid a reporting or recordkeeping obligation, and it does not assist any customer to do so.

13.1 Recordkeeping

The Firm retains AML records — including identification and verification records, beneficial-ownership records, due diligence and risk-rating documentation, transaction and funds-transfer records, alerts, investigations, reporting decisions and the reports themselves — for a minimum of five years from the date of the relevant event, or for such longer period as local law or a litigation hold requires. Records must be complete, retrievable and capable of reconstructing the relationship and the transaction. Records subject to a legal or regulatory hold must not be destroyed under any circumstances.

The Firm complies with funds-transfer recordkeeping and travel-rule requirements, including the obligation to transmit and retain complete originator and beneficiary information, and to identify and address incoming payments with missing or meaningless information.

13.2 Information sharing

- **Section 314(a).** The Firm searches its records against requests from FinCEN on behalf of law enforcement, and responds within the prescribed period. The confidentiality of such requests is absolute; their existence may not be disclosed to the subject or to any unauthorised person, and they may not be used for any purpose other than that permitted.
- **Section 314(b).** The Firm participates in voluntary information sharing with other financial institutions, under the statutory safe harbour, solely for the purpose of identifying and reporting possible money laundering or terrorist financing. All such sharing is authorised, conducted and recorded by FCC. No business may share information under Section 314(b) directly.
- **Intragroup sharing.** Financial-crime information is shared within the Northgate group for AML purposes to the fullest extent permitted by applicable law and data-protection requirements. Where local law restricts such sharing, FCC must be informed and Section 23 applies.

14. Sanctions and Export-Control Interface

Economic sanctions compliance is governed by the Global Sanctions Policy, which is a separate Level 1 policy. Sanctions obligations are strict-liability in nature and are distinct from the risk-based obligations in this Policy; nothing in this Policy may be read as permitting a risk-based approach to a sanctions prohibition.

The two frameworks are nonetheless operationally interdependent. Where information gathered under this Policy — in due diligence, monitoring or investigation — discloses a potential sanctions nexus, evasion typology, or proliferation-financing indicator, it must be escalated immediately to the Global Sanctions Officer as well as to FCC. Conversely, sanctions screening outcomes that indicate potential money laundering must be escalated under this Policy.

15. New Products, New Business and Corporate Transactions

ML/TF risk must be assessed **before** it is assumed — not after launch, and not after close.

- **New products and services.** No new product, service, channel, market, technology or material change to an existing one may be approved or launched without a documented financial-crime risk assessment and the written concurrence of FCC. FCC has the right to withhold concurrence, and a product may not proceed without it.
- **New markets and entities.** Entry into a new jurisdiction, or the establishment of a new legal entity or branch, requires an assessment of the ML/TF risk of that jurisdiction, the adequacy of local supervision, and the Firm’s ability to apply this Policy there.
- **Acquisitions, mergers and portfolio purchases.** Financial-crime due diligence is mandatory in pre-acquisition diligence. The acquiring business must assess the target’s customer base, its historic due diligence, its unreported or unresolved suspicious activity, and its regulatory history. A remediation plan, funded and time-bound, must be approved before close where gaps are identified. Inherited deficiencies become the Firm’s deficiencies on day one.

16. Third Parties, Outsourcing and Intragroup Reliance

The Firm may outsource the performance of activity. It may never outsource the accountability for it.

- Any third party performing an AML-relevant activity for the Firm — including identification and verification, screening, alert review, or investigation support — must be subject to due diligence, contractual obligations that meet this Policy, audit and access rights, and ongoing oversight by the accountable Firm function.
- Reliance on a third party for customer due diligence is permitted only where expressly allowed by applicable law, only where the Firm can obtain the underlying records immediately on request, and only with FCC approval. The Firm remains fully accountable for the adequacy of that diligence.
- Agents, introducers and distributors acting for the Firm must be subject to financial-crime due diligence proportionate to the risk they present, and to contractual termination rights for financial-crime cause.
- Intragroup service arrangements are subject to the same standard. A shared service centre does not dilute the accountability of the business it serves.

17. Technology, Data and Model Governance

The Firm’s AML program depends on the completeness, accuracy, timeliness and lineage of its data. Data quality is a first-line accountability and is subject to independent challenge by FCC.

- Systems used for customer risk rating, screening, monitoring and reporting must have documented coverage: FCC must be able to evidence which products, entities, channels and data feeds are in scope and which are not, and must approve any gap.
- Models and rules-based systems used in the AML program are subject to the Firm’s Model Risk Management Policy, including independent validation, ongoing performance monitoring, and documented change control. Threshold and scenario changes require FCC approval and an assessment of their impact on detection.
- Artificial intelligence and machine-learning techniques may be used to 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.
- Business continuity arrangements must ensure that screening, monitoring and reporting obligations continue to be met during disruption. An outage does not suspend a legal obligation; it creates a backlog that must be worked and, where material, reported.

18. Training and Awareness

Every director, officer, employee and relevant contingent worker must complete AML training on joining and at least annually thereafter. Training is mandatory; completion is tracked; and failure to complete it within the required period is a policy breach, is escalated to the individual’s manager and to Human Resources, and is reflected in performance and compensation outcomes.

- Training content is risk-based and role-specific. Staff in higher-risk roles — correspondent banking, private banking, trade finance, payments, onboarding, and FCC itself — receive deeper, function-specific training informed by the enterprise risk assessment and by real typologies and cases.
- Training must address the individual’s personal obligations, the duty to escalate, the prohibition on tipping off, and the protections available to those who raise concerns.
- The Board and its committees receive training sufficient to enable them to exercise informed oversight and effective challenge.

- FCC assesses the effectiveness of training — not merely its completion — and reports on it to the Financial Crimes Risk Committee.

19. Independent Testing and Assurance

Internal Audit provides independent assurance over the AML program. Testing is performed by individuals who are independent of the design and operation of the controls tested, who are competent in financial crime, and who have unrestricted access to the information they require. Where Internal Audit lacks the necessary specialist expertise, qualified external parties are engaged.

- The scope, frequency and depth of testing is risk-based and informed by, but not limited to, the enterprise risk assessment. Testing must cover program design, operating effectiveness, data integrity, and the adequacy of the second line itself.
- Findings are reported to the Audit Committee, to the Financial Crimes Risk Committee and to the accountable executives, with agreed owners and dates.
- Remediation of findings is tracked to closure and validated independently. Extensions require documented approval. A pattern of extension requests is itself reportable to the Audit Committee.
- Businesses must not obstruct, restrict, influence or attempt to negotiate the substance of an audit finding.

20. Culture, Escalation and Non-Retaliation

A control framework only works in a culture that permits people to use it.

- **Speak up.** Every employee is expected — not merely permitted — to raise financial-crime concerns, through their manager, through FCC, or through the Firm’s confidential and anonymous whistleblowing channels. Concerns may be raised at any time, about anyone, at any level.
- **Non-retaliation.** The Firm strictly prohibits retaliation, in any form, against any person who raises a concern in good faith, who declines to proceed with business on financial-crime grounds, or who cooperates with an internal or external investigation. Retaliation is itself a serious disciplinary offence, up to and including dismissal, and is reported to the Board.
- **Protected disclosures.** Nothing in this Policy, in any employment agreement, in any confidentiality or separation agreement, or in any Firm procedure, limits or may be construed to limit an individual’s right to report a possible violation of law directly to any governmental authority or regulator, including under applicable whistleblower award programs, without notice to or approval from the Firm.
- **Tone from the top and tone from the middle.** Senior and middle managers are assessed on the financial-crime culture within their teams. Commercial pressure that causes staff to feel unable to escalate is a management failure and is treated as such.
- **Incentives.** No performance metric, sales target, incentive plan or discretionary award may be designed or applied in a way that rewards the avoidance, dilution or circumvention of this Policy. Compensation outcomes reflect conduct and control performance, not revenue alone.

21. Consequences of Non-Compliance

Failure to comply with this Policy exposes the Firm to criminal prosecution, civil and criminal monetary penalties, deferred prosecution and consent orders, business restrictions, loss of licences and correspondent access, and severe reputational damage. It exposes individuals to personal criminal liability, personal civil penalties, regulatory prohibition from the industry, and imprisonment.

Any breach of this Policy — including failure to escalate, failure to complete required diligence, falsification or omission of client information, tipping off, obstruction of FCC or Internal Audit, and retaliation against a person who raises a concern — will result in disciplinary action proportionate to the breach, up to and including termination of employment, forfeiture and clawback of unvested and vested compensation, termination of contract, referral to regulators, and referral to law enforcement.

Disciplinary outcomes for financial-crime breaches are reported in aggregate to the Financial Crimes Risk Committee and, for senior individuals, to the Risk Committee of the Board.

22. Policy Governance: Exceptions, Waivers and Breaches

22.1 Ownership and review

The BSA/AML Officer owns this Policy and is accountable for its currency, coherence and enforcement. The Policy is reviewed at least annually, and additionally upon any material change in law, regulation, supervisory expectation, the Firm’s business model, or the Firm’s risk profile. Material amendments require Board approval; non-material and administrative amendments may be approved by the Chief Compliance Officer and are reported to the Risk Committee at its next meeting.

22.2 Exceptions

- An exception to this Policy may be granted only by the BSA/AML Officer, and only where the residual risk is documented, understood, time-bound, mitigated and within appetite.
- The prohibitions in Section 3.1 are absolute and are not capable of exception.
- Every exception must be recorded in the exceptions register, must have an owner and an expiry date, and must be reported to the Financial Crimes Risk Committee. Exceptions do not roll over automatically; they must be re-approved on their merits.
- An exception granted to one business or entity does not create a precedent for any other.

22.3 Breaches

Any known or suspected breach of this Policy must be reported to FCC immediately upon discovery, by the person who discovers it. Concealing a breach, or delaying its reporting to allow it to be corrected first, is itself a breach of this Policy and is treated as an aggravating factor. Material breaches are reported to the Financial Crimes Risk Committee, to the Risk Committee of the Board, and, where required, to the Firm’s regulators.

22.4 Attestation

Each business head and each legal entity chief executive attests annually, in writing, that the business or entity for which they are accountable complies with this Policy, that any exceptions are recorded and within their stated terms, and that any known breaches have been reported. Attestations are supported by evidence and are subject to independent testing. A false or unsupported attestation is a serious disciplinary matter.

23. Conflicts of Law

Where the Firm identifies that compliance with this Policy would require it to breach the law of a jurisdiction in which it operates — for example, where local secrecy, blocking, data-protection or data-localisation law prohibits the collection, retention or transfer of information this Policy requires — the conflict must be escalated immediately to FCC and to Legal. The Firm must not resolve such a conflict unilaterally, locally, or informally.

FCC and Legal will 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 ML/TF risk to an acceptable standard, the Firm will restrict or exit the affected activity. The Firm will not maintain a business it cannot control. All unresolved conflicts of law are reported to the Risk Committee of the Board.

24. Definitions

Term	Meaning as used in this Policy
Beneficial owner	Each natural person who, directly or indirectly, owns or controls a legal entity customer at or above the applicable ownership threshold, and the natural person with significant responsibility for controlling, managing or directing that customer.
BSA/AML Officer	The individual designated by the Board under 31 CFR § 1020.210 as responsible for coordinating and monitoring day-to-day compliance with the Bank Secrecy Act and this Policy; at Northgate, the Global Head of Financial Crimes Compliance.
Customer due diligence (CDD)	The identification and verification of a customer and its beneficial owners, the understanding of the nature and purpose of the relationship, the assignment of a risk rating, and risk-based ongoing monitoring and refresh.
Enhanced due diligence (EDD)	The additional and intensified measures applied to relationships assessed as higher risk, including deeper enquiry into source of funds and source of wealth, senior-management approval, and heightened ongoing scrutiny.
FCC	Financial Crimes Compliance: the second-line function under the BSA/AML Officer responsible for the AML, sanctions, anti-bribery and anti-fraud frameworks.
Money laundering	The process by which the proceeds of criminal conduct are concealed, disguised, converted, transferred or integrated so as to appear legitimate, or by which their true origin, ownership or control is obscured.
Politically exposed person (PEP)	An individual who is or has been entrusted with a prominent public function, together with their immediate family members and known close associates.
Suspicious activity	Any transaction, attempted transaction, instruction or pattern of behaviour that the Firm knows, suspects, or has reason to suspect involves funds derived from illegal activity, is designed to evade a reporting requirement, has no business or apparent lawful purpose, or involves the use of the Firm to facilitate criminal activity.
Terrorist financing	The provision or collection of funds or other assets, by any means, with the intention or knowledge that they are to be used to carry out an act of terrorism or by a terrorist organisation or individual terrorist, irrespective of the lawful or unlawful origin of those assets.
Tipping off	Disclosing, directly or indirectly, to the subject of a suspicious activity report or to any unauthorised person, the fact that such a report has been made, is being considered, or that an investigation is underway.

Appendix A — Principal Regulatory References

The references below are provided for orientation. They do not limit the Firm's obligations, and they are not a substitute for legal advice. Where a reference is amended, superseded or repealed, the obligation as amended applies, and FCC is accountable for reflecting the change in this Policy and in the Standards beneath it.

Citation	Subject
31 U.S.C. §§ 5311–5336	Bank Secrecy Act, as amended by the AML Act of 2020
31 CFR Chapter X	FinCEN implementing regulations
31 CFR § 1020.210	AML program requirements for banks
31 CFR § 1020.220	Customer identification program
31 CFR § 1010.230	Beneficial ownership requirements for legal entity customers
31 CFR §§ 1010.610, 1010.620	Due diligence and enhanced due diligence for correspondent and private banking accounts
31 CFR § 1020.320	Suspicious activity report requirements
31 CFR § 1010.311	Currency transaction report requirements
31 CFR §§ 1010.410, 1010.430	Funds transfer recordkeeping; retention of records
USA PATRIOT Act §§ 311, 312, 313, 314, 319, 326	Special measures; EDD; shell banks; information sharing; foreign bank records; CIP
18 U.S.C. §§ 1956, 1957, 1960	Money laundering; monetary transactions in criminally derived property; unlicensed money transmitting
31 CFR Chapter V	OFAC sanctions regulations
FFIEC BSA/AML Examination Manual	Supervisory examination standard
FinCEN AML/CFT National Priorities	Priorities the program must incorporate
FATF Recommendations (as revised)	International AML/CFT standard applied to non-US operations

Appendix B — Version History and Approval Record

Version	Date	Summary of change	Approved by
9.0	12 Mar 2026	Full rewrite. Added risk appetite and prohibited-activity section; strengthened BSA/AML Officer independence and removal provisions; added technology, data and model governance; added conflicts-of-law protocol; added annual business-head attestation; expanded non-retaliation and protected-disclosure language.	Board of Directors
8.3	1 Apr 2025	Incorporated FinCEN AML/CFT national priorities into the risk-assessment mandate; expanded virtual-asset provisions.	Board of Directors

Version	Date	Summary of change	Approved by
8.2	5 Oct 2024	Clarified FCC authority to decline and exit; added Restricted Business Schedule.	Board of Directors
8.1	3 Apr 2024	Annual review; administrative updates to regulatory references.	Chief Compliance Officer
8.0	29 Mar 2023	Restructure into Level 1 Policy under the Firm’s policy hierarchy; separation of sanctions into a standalone Level 1 policy.	Board of Directors

Approval

This Policy 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.

_____

Chair of the Board of Directors

_____

Chair, Risk Committee of the Board

_____

Chief Executive Officer

_____

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

— End of Policy —