Global AML Operating Procedures

These Procedures set out **how** the requirements of the Global Anti-Money Laundering Policy (Level 1) and the AML Control Framework (Level 2) are executed, step by step, by named roles, within defined service levels. They are mandatory for every person who performs an activity described in them. Where a step cannot be completed as written, the deviation protocol in Section 1.5 applies; the step is never simply skipped.

Document control	Detail
Document title	Global AML Operating Procedures
Classification	Level 3 — Procedure (issued under the Global AML Policy v9.0 and the AML Control Framework v4.1)
Version	6.2 (supersedes 6.1, effective 1 November 2025)
Procedure owner	Head of Financial Crimes Operations
Approved by	Global Head of Financial Crimes Compliance (BSA/AML Officer)
Effective date	1 May 2026
Review cycle	Annual; and on any change to the Policy, the Control Framework, applicable law, or the underlying systems
Systems in scope	NG-KYC (onboarding and CDD workflow); NG-SCREEN (sanctions, PEP and adverse-media screening); NG-DETECT (transaction monitoring); NG-CASE (alert and case management); NG-FILE (regulatory reporting and BSA E-Filing interface); NG-ARCHIVE (records retention)
Applies to	Client Onboarding; KYC Operations; Financial Crimes Investigations; Regulatory Reporting; Screening Operations; Relationship Managers and front-office supervisors; Quality Assurance

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.	How to use these Procedures	1
2.	Roles and hand-offs	2
3.	Customer Identification Program (CIP)	3
4.	Beneficial ownership identification	5
5.	KYC profile: nature, purpose, source of funds and source of wealth	6
6.	Customer risk rating	6
7.	Screening at onboarding and hit disposition	7
8.	Enhanced Due Diligence (EDD)	8
9.	Foreign correspondent banking due diligence	10
10.	Onboarding decision, conditional approval and deferrals	11
11.	Periodic review and event-driven refresh	11
12.	Transaction monitoring: alert handling	12
13.	Investigation standard and case escalation	13
14.	Suspicious Activity Report (SAR) decisioning and filing	15
15.	Currency Transaction Reports and structuring	16
16.	314(a), 314(b), subpoenas and law-enforcement requests	17
17.	Client exit and offboarding	18
18.	Recordkeeping, funds transfers and retention	19
19.	Quality control, quality assurance and management information	19
A.	Appendix A — Consolidated service-level table	21
B.	Appendix B — Alert and case disposition codes	22
C.	Appendix C — Escalation matrix	22

1. How to use these Procedures

1.1 Document hierarchy

Level	Document	Answers
Level 1	Global Anti-Money Laundering Policy	What must be true, and who is accountable
Level 2	AML Control Framework and Risk-Control Matrix	Which controls exist, what they must achieve, how they are tested
Level 3	These Procedures	Who does what, in what order, by when, and with what evidence
Level 4	System work instructions and job aids (NG-KYC, NG-CASE, NG-DETECT)	Which button to press

Where these Procedures conflict with the Policy, the Policy prevails. Where they conflict with a work instruction, these Procedures prevail. Report any conflict to the Procedure owner within one business day of discovery.

1.2 Mandatory language

- **Must** — a mandatory step. Omission is a control failure and a reportable procedure breach.
- **Must not** — a prohibition. There is no risk-based discretion.
- **Should** — the expected approach. A departure must be documented in the case record with the reason.
- **May** — permitted at the discretion of the named role.

1.3 Business-day and clock conventions

Unless stated otherwise, all service levels are expressed in US business days and the clock starts at 00:01 ET on the first business day after the triggering event. Statutory deadlines (SAR, CTR, 314(a), blocked property) are expressed in **calendar** days and are absolute; an internal service level may never be applied in a way that causes a statutory deadline to be missed. Where a statutory deadline falls on a weekend or federal holiday, the filing is made on the preceding business day.

1.4 Four-eyes principle

Every decision that closes risk — clearing a screening hit, closing an alert without escalation, approving a high-risk client, downgrading a risk rating, deciding not to file a SAR — requires a preparer and an independent reviewer of at least one grade senior. The preparer and reviewer must not be the same person, must not report to each other where the decision concerns a relationship they jointly manage, and must be separately recorded in the system of record. Self-review is a control failure regardless of outcome.

1.5 Deviation protocol

1. Stop. Do not complete the activity outside the procedure and document it afterwards.
2. Record the blocked step in NG-CASE with reason code DEV-01 through DEV-06.
3. Escalate to the team lead the same business day. The team lead escalates to the FCC Policy and Standards team within two business days if the deviation is systemic rather than case-specific.
4. Obtain a documented, time-bound deviation approval from the Procedure owner (case-specific) or the BSA/AML Officer (systemic). Approvals expire; they do not roll forward.
5. Log the deviation in the Deviation Register. Deviations are reported monthly to the Financial Crimes Risk Committee with ageing and root cause.

2. Roles and hand-offs

Role	Owns	Does not own
Relationship Manager (RM) / front office	Client information quality and completeness; commercial rationale; responses to Requests for Information within SLA; escalation of unusual behaviour observed in the relationship.	The risk rating. The decision to onboard a high-risk client. The decision to close an alert. Any decision to file or not file a SAR.
KYC Operations Analyst	Collection and verification of CIP and beneficial-ownership evidence; construction of the KYC profile; calculation of the model-driven risk rating; periodic review execution.	Approval of EDD relationships. Any override of the model rating.

Role	Owns	Does not own
Screening Operations Analyst	Level 1 disposition of sanctions, PEP and adverse-media matches within SLA; escalation of true and potential matches.	Release of a blocked or rejected payment. Sanctions determinations, which sit with the Sanctions team.
Financial Crimes Investigator (L2 / L3)	Alert investigation; case build; RFI issuance; investigative conclusion and recommendation; completeness of the case record.	The final SAR decision, which sits with the SAR Review Committee and the BSA/AML Officer.
SAR Review Committee	The decision to file or not to file; narrative approval; continuing-activity decisions; recommendation to exit.	Client communication of any kind.
Regulatory Reporting Team	Timely and accurate filing of SARs, CTRs, blocked-property reports and 314(a) responses; acknowledgement reconciliation; BSA Identifier capture.	The substantive decision to file.
FCC Advisory	Interpretation of the Policy; approval of EDD and restricted business; deviation approvals; the right to decline and exit.	Execution of operational steps, which sits with Operations.
Quality Assurance (QA)	Independent post-completion sampling of all decision types; scoring; theme reporting to the Financial Crimes Risk Committee.	Reworking the case. QA identifies; the accountable team remediates.

The hand-off rule

A hand-off is not complete until the receiving team has accepted the item in the system of record. An item emailed, chased on a call, or verbally agreed is not handed off, the SLA clock does not stop, and accountability remains with the sending team. There are no off-system queues.

3. Customer Identification Program (CIP)

Reference: 31 CFR § 1020.220. No account may be opened, and no transactional access granted, until CIP is complete and verified, save where a documented CIP deferral applies under Section 10.3.

3.1 Minimum identifying information to be collected

Customer type	Information that must be collected before account opening
Natural person (US)	Full legal name; date of birth; residential street address (a P.O. box alone is not acceptable; an APO/FPO or an Army/Air Post Office address is); and a taxpayer identification number (SSN or ITIN).
Natural person (non-US, no TIN)	Full legal name; date of birth; residential street address; and one of: passport number and country of issuance; alien identification card number; or the number and country of issuance of another government-issued document evidencing nationality or residence and bearing a photograph or similar safeguard.
Legal entity (US)	Full legal name; any operating or trade name; principal place of business street address; EIN; state and date of formation; and formation documents (certificate of incorporation, articles of organisation, partnership agreement, trust deed, or equivalent).
Legal entity (non-US)	As above, substituting the local registration number and register; and, where no TIN exists, a government-issued number evidencing the existence of the entity. A certified or apostilled translation is required for documents not in English.

Customer type	Information that must be collected before account opening
Trusts, foundations and similar arrangements	The trust instrument; and the identity of the settlor, trustee(s), protector (if any), named beneficiaries or class of beneficiaries, and any other natural person exercising ultimate effective control.

3.2 Verification

Identity must be verified within a reasonable time — at Northgate, **before** account opening for all customers other than those subject to an approved deferral, and in no case later than **30 calendar days** after account opening. Verification is performed documentarily, non-documentarily, or both, on a risk basis. Higher-risk customers require both.

Documentary verification — acceptable evidence

- Individuals: unexpired government-issued photographic identification bearing name and, where available, address — passport, driver's licence, state identification card, permanent resident card, military identification, or national identity card.
- Entities: certified certificate of incorporation or good standing dated within 90 days; articles; partnership or trust deed; corporate resolution or board mandate identifying authorised signatories; and evidence of the registered and operating addresses.
- Documents must be legible, unexpired, and free of alteration. A copy is acceptable only where it is certified, notarised, apostilled or captured through an approved digital identity channel with liveness detection.

Non-documentary verification — acceptable methods

- Comparison of the information provided against an independent, reputable reference database (credit bureau, public registry, commercial identity provider).
- Verification of references with other financial institutions.
- Obtaining a financial statement, audited accounts, or a bank reference for an entity.
- Micro-deposit or account-ownership confirmation against a verified funding account.

CIP failure

Where the Firm cannot form a reasonable belief that it knows the true identity of the customer, the analyst must not open the account; must close a provisionally opened account and return funds only to the verified source; must not process outbound transactions; must refer the matter to Financial Crimes Investigations to determine whether a SAR is warranted; and must not disclose to the customer that a referral has been made. Record disposition code CIP-FAIL and escalate to the team lead the same day.

3.3 CIP execution steps

1. Receive the onboarding request in NG-KYC. Confirm the entity type, jurisdiction of incorporation or residence, and the products requested. Product set drives the diligence path.
2. Collect the minimum identifying information in Section 3.1. Do not proceed with partial data; return the request to the RM with reason code RFI-CIP and a specified gap list.
3. Verify identity by the method(s) required for the risk band. Attach every source document to the NG-KYC record; screenshots of a screen are not evidence unless system-generated and timestamped.

4. Screen the customer and all related parties (Section 7) **before** the record is passed for approval.
5. Record the CIP outcome (PASS / FAIL / DEFERRED) with the analyst identifier and timestamp. A second analyst reviews and confirms the record under the four-eyes principle.
6. Retain all CIP records for five years after the account is closed (31 CFR § 1020.220(a)(3)).

4. Beneficial ownership identification

Reference: 31 CFR § 1010.230. Applies to every legal entity customer at account opening and on every trigger event thereafter.

4.1 The two prongs

Prong	Who must be identified	Threshold
Ownership prong	Each natural person who, directly or indirectly, owns or controls equity interests in the legal entity customer.	25% or more. Northgate applies a **10%** internal threshold for customers rated High risk, for customers in high-risk jurisdictions, and for private banking relationships.
Control prong	A single natural person with significant responsibility to control, manage or direct the entity — e.g. chief executive officer, chief financial officer, chief operating officer, managing member, general partner, president, vice president, treasurer, or any other individual who performs similar functions.	Always exactly one individual must be named, even where the ownership prong yields no one.

For each beneficial owner identified, collect and verify name, date of birth, residential address and TIN (or passport number and country for non-US persons) to the same standard as a natural-person customer under Section 3. Identity of a beneficial owner is verified; **status** as a beneficial owner may be certified by the individual opening the account.

4.2 Layered and indirect ownership

1. Obtain a complete ownership structure chart, dated and signed by an authorised officer, showing every layer from the customer to the ultimate natural persons.
2. Calculate indirect ownership multiplicatively through each layer (e.g. a natural person owning 60% of an intermediate holding company that owns 50% of the customer holds 30% indirectly and is in scope).
3. Where the chain terminates in a listed company, a regulated financial institution, a government body, or another exempt entity, record the exemption and its basis and stop the look-through at that point.
4. Where the chain terminates in a trust, a nominee arrangement, or a bearer-share entity, escalate to FCC Advisory. Bearer-share entities are prohibited under Policy § 3.1.
5. Where the structure cannot be resolved to natural persons — or where the explanation for its complexity is not credible — do not onboard. Escalate to FCC Advisory and refer to Investigations for a suspicion assessment.

4.3 Refresh triggers for beneficial ownership

- Any new account opened by an existing legal entity customer (a certification must be obtained or re-affirmed).
- Any change of ownership, control, directors, or authorised signatories notified to or detected by the Firm.

- Any adverse media, sanctions or PEP match against a person in the ownership chain.
- Any periodic review under Section 11.
- Any information that causes the Firm to doubt the accuracy of a previously obtained certification. Doubt — not proof — is the trigger.

5. KYC profile: nature, purpose, source of funds and source of wealth

The KYC profile is the document against which all future activity is judged. A weak profile guarantees a weak alert. It must state what the customer does, why it banks with Northgate, and what its activity is expected to look like — specifically enough that a deviation would be visible.

5.1 Mandatory profile fields

Field	Standard	Unacceptable
Nature of business	Specific activity, industry code, products sold, customer base, geographies of operation and counterparties.	“Consulting.” “General trading.” “Investments.”
Purpose of the relationship	The products requested and the business need each serves.	“Banking services.”
Expected activity	Expected monthly volume and value, by product and channel; expected cash use; expected counterparty countries; expected wire corridors; seasonality.	Blank fields, or a single figure with no basis.
Source of funds (SOF)	The origin of the money that will move through **this account** — the specific activity, payer, contract or transaction that generates it.	“Business income.” “Savings.”
Source of wealth (SOW)	How the customer’s **overall wealth** was accumulated, over time, with corroboration — sale of a business (with sale agreement), inheritance (with probate), employment (with contract or filings), investment returns (with statements).	“Inherited.” “Successful businessman.” Any SOW asserted without a corroborating document for a High-risk or PEP relationship.

5.2 SOF / SOW corroboration standard by risk band

Risk band	SOF	SOW
Low	Stated and plausible against the business profile.	Not required unless a trigger arises.
Medium	Stated, plausible and internally consistent with expected activity.	Stated; documentary corroboration on a sample basis.
High	Stated and corroborated with at least one independent document per material funding stream.	Stated and corroborated with independent documentary evidence covering the material components of wealth.
PEP / private banking	Corroborated for every funding stream; unexplained third-party funding is a bar to onboarding.	Full documented wealth narrative with independent corroboration, reviewed by FCC Advisory and approved by senior management (Policy § 11).

6. Customer risk rating

Every customer carries a risk rating produced by the NG-KYC rating model. The model is owned by FCC, validated under the Model Risk Management Policy, and is the only permitted method. Analysts must not compute

a rating by judgement, spreadsheet, or precedent.

6.1 Rating factors and indicative weights

Factor	Weight	Illustrative drivers
Customer type and legal structure	20%	Natural person; operating company; holding company; trust; foundation; MSB; VASP; correspondent bank; charity; embassy; complexity and opacity of the structure; nominee use.
Country risk	25%	Country of incorporation, of operation, of the beneficial owners, and of expected counterparties. Driven by the FCC Country Risk List (FATF listings, sanctions exposure, corruption and secrecy indices, narcotics and trafficking exposure, and Northgate's own SAR experience).
Product and service risk	20%	Cash-intensive products; international wires; trade finance; correspondent accounts; payable-through and nested activity; private banking; custody and omnibus; virtual assets; prepaid and stored value.
Channel risk	10%	Face-to-face; digital non-face-to-face with liveness; introduced via a third party; agent or intermediary; white-label.
Anticipated activity	15%	Expected cash volume; expected cross-border volume and corridors; velocity; round-dollar and third-party payment expectation.
Screening and adverse information	10%	PEP status (self, family, close associate); sanctions nexus in the ownership chain; adverse media relevance and recency; prior SAR history; prior exit by the Firm or another institution.

6.2 Bands, and what the band drives

Band	Score	Refresh	Diligence	Monitoring
Low	0–39	36 months	Standard CDD	Standard scenarios; standard thresholds
Medium	40–69	24 months	Standard CDD plus SOF corroboration	Standard scenarios; tightened thresholds
High	70–89	12 months	EDD (Section 8); senior approval	Enhanced scenario set; reduced thresholds; periodic activity review
Prohibited / Unacceptable	90+	n/a	Do not onboard; exit if existing	Escalate to FCC Advisory and Investigations immediately

6.3 Overrides

- **Upward override** (rating increased above the model output) may be applied by any KYC analyst, investigator or RM at any time, with a recorded reason. It requires no approval. Raising risk is always permitted.
- **Downward override** (rating reduced below the model output) requires written justification, evidence, and approval by FCC Advisory at Vice President level or above. It must never be applied to resolve a commercial impasse, to meet an onboarding service level, or because the customer objects to the rating.
- All overrides are logged, aged, and reported monthly. A downward override rate above the tolerance in the KRI dashboard triggers a thematic review by QA.
- A rating must never be downgraded while an alert, an investigation, or an unfiled suspicion assessment is open on the relationship.

7. Screening at onboarding and hit disposition

Screening is performed in NG-SCREEN against: OFAC SDN and Consolidated Non-SDN lists; other applicable sanctions regimes (UN, EU, UK OFSI, and local lists relevant to the booking entity); PEP data; adverse media; and internal watchlists (prior exits, prior SAR subjects, known fraud).

7.1 Who is screened

- The customer; all beneficial owners identified under Section 4; the control-prong individual; directors and authorised signatories; and, for trusts, the settlor, trustee, protector and known beneficiaries.
- Related parties: guarantors, powers of attorney, and — for trade finance — all named parties to the underlying transaction, plus vessels, ports and goods.
- Screening is performed at onboarding, on every list update, on every change to a screened party, and on a continuous basis for the whole customer base thereafter.

7.2 Disposition SLAs and outcomes

Match type	Disposition SLA	Action
Sanctions — potential true match	Immediate; within 2 hours of alert generation	Freeze the onboarding and any pending payment. Escalate to the Sanctions team without clearing. Do not contact the customer. The Sanctions team makes the blocking or rejection determination; blocked property is reported to OFAC within 10 business days.
Sanctions — false positive	Same business day	Clear with documented discriminators (full DOB, full name, nationality, identifier mismatch). “Looks different” is not a discriminator. Four-eyes review required.
PEP — confirmed	2 business days	Set PEP flag; route to EDD (Section 8). Do not clear a PEP flag to accelerate onboarding. Removal of a PEP flag requires FCC approval and documented evidence that the person is not, and is no longer connected to, a prominent public function.
Adverse media — relevant	3 business days	Assess relevance (is it the same person?), materiality (does it concern financial crime, corruption, sanctions, violence, or predicate offences?) and recency. Material and relevant findings route to EDD and may route to Investigations.
Internal watchlist hit	1 business day	Route to FCC Advisory. A previously exited customer must not be re-onboarded without BSA/AML Officer approval.

Clearing standard

A screening hit is cleared on evidence, never on inference and never on time pressure. The clearing rationale must name the specific data points that differ between the customer and the listed party, and must be capable of being understood by an examiner two years later with no other context. If the analyst cannot write that sentence, the hit is not a false positive and must be escalated.

8. Enhanced Due Diligence (EDD)

8.1 Triggers

- A High risk rating from the model, or any upward override to High.
- PEP status of the customer, a beneficial owner, a controller, or an immediate family member or known close associate.
- Any relationship in a jurisdiction rated High on the FCC Country Risk List.

- Foreign correspondent banking (Section 9) and foreign private banking accounts (31 CFR § 1010.620).
- Any customer in a category on the Restricted Business Schedule — MSBs, VASPs, cash-intensive businesses, gaming, precious metals and stones, embassies and foreign missions, charities operating in conflict zones, arms and dual-use goods.
- Material, relevant and recent adverse media concerning financial crime.
- Complex, opaque or unexplained ownership; nominee arrangements; multi-layer offshore structures.

8.2 EDD steps

1. Complete all standard CDD first. EDD is additive; it does not replace any standard step.
2. Obtain and corroborate SOW and SOF to the High or PEP standard in Section 5.2.
3. Obtain audited financial statements (or equivalent) for the last two years for corporate customers; and the ownership chart certified within the last 12 months.
4. Perform an enhanced negative-news search over at least 10 years, in the local language of each material jurisdiction, using approved research tools. Document the search terms, the databases used, the date, and the results — including nil results.
5. Where the relationship involves a High-risk jurisdiction, document the specific rationale for the Firm's involvement and the expected corridors.
6. Where the counterparty set is material, screen and profile the customer's principal counterparties.
7. Prepare the EDD memorandum: profile, structure, SOW/SOF, adverse findings and their resolution, residual risk, proposed mitigants, and a clear recommendation.
8. Obtain approvals per Section 8.3. Approval must be recorded in NG-KYC, not in email.
9. Set the enhanced monitoring flag, which reduces detection thresholds and adds the enhanced scenario set, and schedule the 12-month refresh.

8.3 Approval authority

Relationship	Recommender	Approver
High risk (standard)	KYC Operations, VP	FCC Advisory, Director
PEP (domestic or foreign, non-private-banking)	FCC Advisory, Director	Business Head + FCC Managing Director
Senior foreign political figure, private banking	FCC Advisory, Managing Director	Financial Crimes Risk Committee; annual re-approval required
Foreign correspondent bank, standard risk	Correspondent Banking Compliance	FCC Advisory, Managing Director
Foreign correspondent bank in a High-risk jurisdiction; or with nesting exposure	FCC Advisory, Managing Director	Financial Crimes Risk Committee
Any customer on the Restricted Business Schedule	Per the Schedule	Per the Schedule; never below Director

Approval is not a formality

An approver who approves an EDD relationship personally attests that they have read the memorandum, that the residual risk is within appetite, and that the Firm can control it. Approvals are sampled by QA and tested by Internal Audit. An approver who cannot explain the basis of an approval at testing is the subject of the finding.

9. Foreign correspondent banking due diligence

References: USA PATRIOT Act §§ 312, 313, 319; 31 CFR §§ 1010.610, 1010.630, 1010.670.

9.1 Mandatory information set

- A completed and signed Wolfsberg Correspondent Banking Due Diligence Questionnaire (CBDDQ), dated within 12 months, together with the respondent's AML policy, sanctions policy, and most recent independent AML audit or examination summary.
- The USA PATRIOT Act Certification regarding Correspondent Accounts for Foreign Banks, including the shell-bank certification and the designation of an agent for service of process in the United States (§ 319(b)).
- Ownership and control of the respondent, including any state ownership, and screening of its owners, directors and senior management.
- The nature and quality of supervision in the respondent's home jurisdiction, and whether it operates under an offshore banking licence.
- The respondent's customer base, products, and the markets it serves; the expected volume, value, currency and corridors of activity through the Northgate account.
- Whether the respondent permits **nested** or downstream correspondent activity, and if so, which institutions, in which jurisdictions, and under what controls.
- Whether the account will be used as a **payable-through** account, and if so, the identity and diligence status of the underlying customers with transactional access.

Absolute prohibitions in correspondent banking

No account may be opened, maintained, administered or managed for a foreign shell bank, or for any foreign bank that permits its account to be used by a foreign shell bank (§ 313). No payable-through arrangement may be permitted where the underlying customers are not identified and subject to due diligence. Where a respondent is unable or unwilling to identify its nested institutions, the nesting must be prohibited contractually and monitored for, or the relationship must be exited. These are not risk-based judgements.

9.2 Ongoing requirements

- Annual refresh of the CBDDQ, the certification, and the risk assessment; 12-month refresh for High-risk respondents, with a mid-cycle activity review at six months.
- Monthly review of actual versus expected activity by corridor, currency, volume and value. Material unexplained variance is an escalation trigger, not a data-quality note.
- Continuous monitoring for nesting indicators: originators and beneficiaries inconsistent with the respondent's stated customer base; third-country flows; MT202COV cover payments inconsistent with the underlying

MT103; sudden new corridors.

- Response to a § 319(b) request from the Secretary of the Treasury or the Attorney General within **7 calendar days**. Failure to produce records may require termination of the relationship within 10 business days of written notice.

10. Onboarding decision, conditional approval and deferrals

10.1 Decision

The onboarding decision is recorded in NG-KYC as APPROVED, APPROVED WITH CONDITIONS, DECLINED, or WITHDRAWN. A decision is only valid where the CIP, beneficial ownership, KYC profile, risk rating, screening disposition and (where applicable) EDD steps are all complete and evidenced in the record. NG-KYC enforces this; analysts must not seek to bypass the workflow through manual account opening in the core banking system. Any account opened outside NG-KYC is a control breach and must be reported within one business day.

10.2 Conditional approval

A relationship may be approved subject to conditions — for example, restricted products, a cash prohibition, corridor restrictions, volume caps, or a shortened review cycle. Conditions must be specific, systemically enforceable, owned by a named individual, and monitored. A condition that cannot be enforced by a system control must not be used as the basis for approval.

10.3 CIP and CDD deferrals

Rule	Detail
Who may grant	FCC Advisory at Director level or above. No business or RM may grant a deferral. No deferral may be granted by email.
Maximum period	30 calendar days from account opening, and never beyond the statutory CIP limit. No extension is permitted; a second deferral on the same relationship is prohibited.
Not available for	PEPs; High-risk customers; correspondent banks; any Restricted Business Schedule category; any customer with an unresolved screening hit; beneficial ownership identification (never deferrable).
Restrictions during deferral	Account is credit-only or blocked for outbound activity, as determined by FCC. No wires out. No cash. No new products.
On expiry	If the outstanding item is not received, the account is restricted automatically at day 30 and exit is initiated under Section 17. Investigations assesses whether a SAR is warranted.
Reporting	All deferrals are logged, aged, and reported weekly to the Head of Financial Crimes Operations and monthly to the Financial Crimes Risk Committee.

11. Periodic review and event-driven refresh

11.1 Cadence

Risk band	Cycle	Start of outreach	Escalation if incomplete
High / PEP / correspondent	12 months	90 days before due date	Day 0 overdue: RM and business head notified. Day 30: account restricted. Day 60: exit initiated.
Medium	24 months	60 days before due date	Day 30 overdue: escalation to business head. Day 60: account restricted. Day 90: exit initiated.
Low	36 months	45 days before due date	Day 60 overdue: escalation. Day 120: restriction and exit assessment.

Overdue reviews are a reportable KRI. The population of customers whose review is overdue beyond the restriction point must be zero; any exception requires BSA/AML Officer approval and is reported to the Financial Crimes Risk Committee by name.

11.2 Event-driven triggers (non-exhaustive)

- A change in beneficial ownership, control, directors, signatories, legal name or jurisdiction.
- A new sanctions, PEP or material adverse-media match on any screened party.
- The filing of a SAR on the relationship (a review is mandatory within 30 days of filing).
- Sustained activity materially inconsistent with the KYC profile — volume, value, counterparties, corridors or cash use.
- A new product or a new country of activity being added to the relationship.
- A request to remove a restriction or condition imposed at onboarding.
- The customer’s designation as a PEP after onboarding, including by promotion or election.
- Notification that another financial institution has exited the customer.

11.3 What a review must actually do

A periodic review is not a document-refresh exercise. The reviewer must compare **actual** activity over the review period against the **expected** activity recorded in the profile, and must explain the variance. Where activity is materially inconsistent with the profile and no credible explanation exists, the reviewer must refer the relationship to Investigations before the review is closed. A review closed as “no change” where activity has clearly changed is a QA failure and a control breach.

12. Transaction monitoring: alert handling

NG-DETECT runs scenario-based detection on a T+1 batch cycle across all in-scope products, supplemented by intraday rules for cash and wire activity. Scenario coverage, segmentation and thresholds are governed by the AML Control Framework (Level 2) and the Model Risk Management Policy; they are not adjustable by operations.

12.1 Alert lifecycle and service levels

Stage	Owner	SLA	Purpose
Generation and enrichment	NG-DETECT (automated)	T+1 by 06:00 ET	Alert created, deduplicated, linked to the customer, enriched with KYC profile, prior alert and prior SAR history, and assigned a priority score.

Stage	Owner	SLA	Purpose
L1 triage	Financial Crimes Analyst	5 business days from assignment	Rule out obvious false positives against the profile and known activity. Close with rationale, or escalate. L1 may not close an alert on a customer with a prior SAR in the last 12 months — that alert routes directly to L2.
L2 investigation	Financial Crimes Investigator	30 calendar days from alert creation	Full investigation to the standard in Section 13. Conclude: close with rationale; or escalate to L3 / SAR recommendation.
L3 case	Senior Investigator	60 calendar days from alert creation	Complex, multi-jurisdiction, multi-entity, or SAR-recommended matters. Produce the case file and the draft narrative.
SAR decision	SAR Review Committee	Within the statutory clock (Section 14)	File or do not file. Both outcomes are documented decisions.

The 30-day clock is not the SLA clock

Internal SLAs (5 / 30 / 60 days) exist to ensure the statutory SAR deadline is met, not to define it. The statutory clock starts on the date of **initial detection of facts that may constitute a basis for filing** — which is frequently the alert date, and is sometimes earlier. Investigators must record the initial-detection date explicitly on the case; it is the single most-tested date in any BSA examination. An investigation running long does not extend it.

12.2 Prioritisation

- Alerts are worked in priority order, not in date order. Priority is driven by customer risk band, scenario severity, value, prior SAR history, sanctions or terrorism nexus, and vulnerable-customer indicators.
- Any alert with a potential terrorist-financing, human-trafficking, child-exploitation or sanctions-evasion indicator is escalated **immediately** to a Senior Investigator, regardless of value and regardless of queue position. These do not wait for triage.
- Ageing is measured from alert creation, never from assignment. Re-assignment does not reset the clock. Backlog above tolerance is a KRI breach and is reported to the Financial Crimes Risk Committee.

12.3 Prohibited alert-handling practices

- Closing an alert because the customer is long-standing, profitable, well-known, or personally known to the analyst or the RM.
- Closing an alert because a prior similar alert was closed. Each alert is assessed on its own facts; a prior closure is context, never a rationale.
- Closing an alert on the strength of an RM’s verbal assurance that the activity is “fine”. RM input is evidence to be tested, not a conclusion to be adopted.
- Bulk-closing alerts to meet a backlog target, or closing alerts without opening the underlying transaction data.
- Asking the customer to explain activity in a way that discloses that they are under review (see Section 13.3).

13. Investigation standard and case escalation

13.1 Minimum investigative steps

1. Establish the **initial detection date** and record it. Everything else follows from it.

2. Review the KYC profile: who is the customer, what do they do, what was expected?
3. Pull the transaction data for a minimum **90-day lookback** from the alert date; extend to 12 months where the pattern is periodic, structured, or the customer is High risk; extend further where the activity appears to be a continuation.
4. Analyse the flow: source, path, destination. Identify originators, beneficiaries, counterparties, intermediaries, corridors, and the relationship between them. Look for circularity, layering, pass-through, round amounts, just-under-threshold values, and rapid in-and-out movement.
5. Review linked parties: related accounts, shared addresses, shared phone numbers, shared devices, shared signatories, common counterparties.
6. Screen all newly identified counterparties.
7. Search adverse media and public records on the customer and material counterparties.
8. Issue a Request for Information (RFI) to the RM where the commercial rationale is unclear (Section 13.3).
9. Reach a conclusion, state it in writing, and support it with the evidence in the case file. The conclusion must answer: is there a reasonable basis to suspect that these funds derive from illegal activity, are designed to evade a reporting requirement, have no apparent lawful purpose, or facilitate criminal activity?

13.2 Documentation standard

The case file must be capable of being read, understood and re-performed by an independent reviewer — an examiner, an auditor, or a court — with no other context and no access to the investigator. It must contain: the alert(s); the KYC profile as at the time; the transaction data analysed; every search performed and its result, including nil results; every RFI and response; the analysis; the conclusion; the decision; and the names, roles and timestamps of the preparer and reviewer.

- Write conclusions in complete sentences. “Activity consistent with profile” is not a conclusion; it is an assertion. State **which** activity, **which** part of the profile, and **why** they are consistent.
- Do not record legal conclusions (“the customer committed fraud”), speculation, opinions about the customer, or anything that would not survive disclosure.
- Do not delete or overwrite. Case records are append-only and are subject to legal hold.

13.3 Requests for Information (RFI) — and the tipping-off boundary

Rule	Detail
Who may be asked	The Relationship Manager or the front-office supervisor, through NG-CASE. Never the customer directly by the investigator.
RM response SLA	5 business days. Non-response escalates to the business head at day 6 and to the Financial Crimes Risk Committee at day 15. Persistent non-response is a conduct matter.
What the RM may be told	That information is required for a periodic or regulatory review. The RM must never be told that a SAR is being considered, investigated or filed.
Customer contact	Where the customer must be asked (e.g. for an invoice or a contract), the request must be framed as routine account maintenance or a periodic review, must be pre-approved by the investigator’s team lead, and must never reference an alert, an investigation, a report, law enforcement, or unusual activity.

Rule	Detail
If the customer asks directly	Do not confirm or deny. State that the Firm periodically reviews account information. Notify FCC immediately and record the interaction in NG-CASE.

Tipping off

Disclosing the existence, contents, or contemplation of a SAR to the subject or to any unauthorised person may be a federal criminal offence (31 U.S.C. § 5318(g)(2)). This includes hints, tone, a sudden change in service, an unexplained request for documents framed as urgent, and any statement that "compliance is asking questions." If in doubt, say nothing and call FCC.

14. Suspicious Activity Report (SAR) decisioning and filing

Reference: 31 CFR § 1020.320. A SAR is required where the Firm knows, suspects, or has reason to suspect that a transaction conducted or attempted by, at, or through the Firm involves funds derived from illegal activity or is intended to disguise such funds; is designed to evade the BSA or its regulations, including by structuring; has no business or apparent lawful purpose and the Firm knows of no reasonable explanation after examining the available facts; or involves the use of the Firm to facilitate criminal activity — and the transaction involves or aggregates **$5,000 or more** in funds or other assets.

Note that **attempted** transactions are reportable, and that no dollar threshold applies to insider abuse. A customer who abandons a transaction when asked for information has attempted it.

14.1 Statutory deadlines

Situation	Deadline
Suspect identified	File within **30 calendar days** of the initial detection of facts that may constitute a basis for filing.
No suspect identified	The Firm may take an additional 30 days to identify a suspect, but must file no later than **60 calendar days** after initial detection.
Continuing activity	Where suspicious activity continues, file a continuing-activity report no later than **120 calendar days** after the date of the previously related filing. Review the relationship at each 90-day point to determine whether continuing activity exists.
Situations requiring immediate attention	Where the activity involves an ongoing violation, terrorist financing, or requires immediate attention, notify law enforcement and the Firm's primary federal regulator **immediately** by telephone, in addition to filing. Immediate notification does not relieve the Firm of the obligation to file.

14.2 Decision process

1. The investigator submits the case with a recommendation (FILE / NO FILE) and a draft narrative.
2. The SAR Review Committee — chaired by the Head of Financial Crimes Investigations, with FCC Advisory and Legal in attendance — meets at least twice weekly and ad hoc for time-critical matters.
3. The Committee decides on the facts alone. No business representative attends; no commercial information is presented; the identity of the RM and the revenue of the relationship are not before the Committee.

4. Both outcomes are documented. A NO FILE decision is recorded with the reasoning, is reviewed by QA at a minimum sampling rate of 10%, and is tested by Internal Audit. “No file” is a decision, not an absence of one.
5. The BSA/AML Officer, or a delegate at Managing Director level, approves the final filing. The BSA/AML Officer may direct a filing over a Committee decision not to file; no one may direct the BSA/AML Officer not to file.

14.3 Narrative standard

The narrative is the SAR. A complete narrative answers **who, what, when, where, why and how**, in chronological order, in plain English, with no unexplained abbreviations, no internal jargon, no system codes and no acronyms that a law-enforcement reader would not know.

- **Who:** the subject(s), with full identifiers — name, DOB, address, TIN/passport, occupation, account numbers, and their relationship to each other.
- **What:** the instruments and mechanisms — cash, wires, cheques, ACH, virtual assets — with dollar amounts and totals.
- **When:** the date range of the activity, and the initial detection date.
- **Where:** the branches, jurisdictions, corridors, and the location of any beneficiary.
- **Why:** why the Firm considers the activity suspicious — the specific red flags, expressed against the customer’s known profile and expected activity.
- **How:** the mechanics of the pattern, described so that a reader can follow the money.
- State clearly whether the Firm has closed or will close the account, and whether the Firm has filed previously on this subject (with the prior BSA Identifier).
- Do not include the SAR form data itself in the narrative; do not speculate; do not use conditional language to hedge a suspicion the Firm actually holds.

14.4 Filing, confidentiality and supporting documentation

- Filing is made through the FinCEN BSA E-Filing System by the Regulatory Reporting team. The BSA Identifier acknowledgement is retrieved, reconciled against the case, and stored in NG-FILE. An unreconciled acknowledgement is a reportable control failure.
- The SAR and all supporting documentation are retained for **five years** from the date of filing. Supporting documentation is deemed to be filed with the SAR and must be produced to FinCEN or an appropriate law-enforcement or supervisory agency on request — without a subpoena.
- Access to SAR data is restricted on a strict need-to-know basis, is logged, and is reviewed. SARs are not stored on shared drives, are not emailed outside FCC, and are not discussed in open-plan settings.
- The Board is informed of SAR filings in aggregate, and of individually significant filings by exception, in a manner that preserves confidentiality.

15. Currency Transaction Reports and structuring

15.1 CTR requirements

Rule	Detail
Trigger	Currency transactions in excess of **$10,000** conducted by, or on behalf of, the same person, in or out, on the same business day.
Aggregation	Multiple transactions are aggregated where the Firm has knowledge that they are by or on behalf of the same person and total more than $10,000 in the same day. Aggregation is systemic in NG-DETECT and is not a manual judgement.
Deadline	File within **15 calendar days** of the transaction date (25 days if filed on magnetic media, which Northgate does not use).
Identification	Verify and record the identity of the person conducting the transaction and the person on whose behalf it is conducted, including a valid identification document and TIN.
Exemptions	Phase I (banks, government agencies, listed companies and their subsidiaries) and Phase II (eligible non-listed businesses and payroll customers) exemptions are administered centrally by Regulatory Reporting via a DOEP filing, reviewed annually, and are never granted by a branch.
Corrections	An error identified after filing is corrected by an amended CTR promptly. Systemic errors are escalated as a control failure, root-caused, and reported with a backfiling plan.

15.2 Structuring

Structuring — breaking a transaction into smaller amounts to evade the reporting threshold — is a federal crime (31 U.S.C. § 5324) and is reportable on a SAR irrespective of whether the underlying funds are legitimate. Legitimate money can be criminally structured.

- Staff **must not** advise, hint, coach or assist a customer to avoid the reporting threshold — including by suggesting they deposit less, split the transaction, come back tomorrow, or use another branch. This is a criminal offence and results in dismissal.
- Where a customer, on being informed of the reporting requirement, reduces or abandons the transaction, staff must complete the transaction as originally presented if it has already occurred, must not offer an alternative, must record the interaction, and must escalate to FCC the same day. This is a classic reportable pattern and it is an attempted transaction.
- Detection scenarios cover: multiple sub-threshold cash deposits across branches, ATMs and days; deposits just below $10,000 by design; and use of multiple individuals to conduct related transactions (smurfing).

16. 314(a), 314(b), subpoenas and law-enforcement requests

Request type	Handling
FinCEN 314(a)	Requests are collected from the secure FinCEN website on the prescribed cycle. The Firm must search its records for the named subjects and respond within **14 calendar days**. Scope: accounts maintained during the preceding 12 months, and transactions conducted during the preceding 6 months, unless the request specifies otherwise. A positive match is reported through the secure website. The Firm must not use the request as the sole basis for a SAR — but a match is a trigger to review the relationship and to consider whether a SAR is independently warranted. The request is strictly confidential; the subject must never be contacted, and the request must not be used for any other purpose (e.g. credit or marketing decisions).
314(b) voluntary sharing	Only FCC may share or receive information under the 314(b) safe harbour, only with institutions whose registration with FinCEN has been verified within the last 12 months, only for the purpose of identifying and reporting possible money laundering or terrorist financing, and only where the Firm's own registration is current. Each exchange is logged. Businesses must never share directly.

Request type	Handling
Grand jury subpoena, administrative subpoena, National Security Letter	Route immediately to Legal and FCC. Do not respond directly and do not notify the customer. An NSL carries a non-disclosure obligation; the very existence of the letter must not be revealed. Receipt of a subpoena is a trigger to review the relationship and to consider a SAR independently — the subpoena itself is not the SAR.
§ 319(b) foreign bank records request	Produce records within **7 calendar days**. Failure to comply may require termination of the correspondent relationship within 10 business days of written notice from the Secretary or the Attorney General.
Keep-open letter from law enforcement	Accept only in writing, from a supervisory-level official, specifying the account, the duration and the purpose. Route to Legal. The letter does not relieve the Firm of its obligation to file, and to continue to file, SARs on the activity.

17. Client exit and offboarding

17.1 Grounds and decision

Exit is recommended by FCC Advisory or Investigations and decided by FCC. The business may make representations to the Financial Crimes Risk Committee; it may not veto, delay or relitigate the decision (Policy § 3.3). Exit decisions must be based on the ML/TF risk of the specific relationship, not on the category, nationality or lawful line of business of the customer.

17.2 Sequence

1. Before any exit communication, Investigations must determine whether a SAR is required. Where it is, the SAR is filed **before or contemporaneously with** the exit — never after the customer has been notified.
2. FCC determines the exit method: immediate closure and blocking (where continued service would facilitate crime), or an orderly wind-down over 30, 60 or 90 days.
3. Legal reviews for contractual notice obligations, ongoing credit exposure, and jurisdictional restrictions on closure.
4. The RM issues the exit notification using the approved template. The notification must state no reason beyond a commercial decision, must never reference compliance, financial crime, a report, a review, or law enforcement, and must never be varied by the RM.
5. Funds are returned only to the verified source account in the customer's name. Do not remit to a third party, to a new institution nominated at the point of exit, or to a jurisdiction inconsistent with the profile, without FCC approval.
6. Add the customer and its beneficial owners to the internal watchlist. Re-onboarding requires BSA/AML Officer approval.
7. Continue monitoring the account until closure. Suspicious activity during wind-down is reportable and may require a continuing-activity SAR.
8. Retain all records for five years from the date of closure.

Never explain an exit

The single most common tipping-off breach at any bank is a well-meaning relationship manager explaining to a valued client why the relationship is ending. There is no form of words that safely conveys "we filed a report." The approved template says nothing, deliberately. Do not improvise, do not apologise for the compliance function, and do not offer to "see what I can do."

18. Recordkeeping, funds transfers and retention

Record	Requirement	Retention
CIP records	Identifying information; description of the documents relied on; the methods and results of non-documentary verification; the resolution of any discrepancy.	5 years after the account is closed
Beneficial ownership	Certification form; identifying information; verification evidence; ownership charts.	5 years after the account is closed
Funds transfers of **$3,000 or more**	Transmittal order records: name and address of the transmittor and recipient; the amount; the execution date; the payment instructions; the identity of the recipient's financial institution; and the account numbers. Complete originator and beneficiary information must be transmitted with the payment (the Travel Rule).	5 years from the date of the transaction
SARs and supporting documentation	The filed report; the case file; the decision record; the BSA Identifier.	5 years from the date of filing
CTRs	The filed report and the identification evidence.	5 years from the date of filing
Monetary instruments $3,000–$10,000 in cash	Contemporaneous log of the purchaser, the instrument and the identification presented.	5 years
Training records	Content, attendees, dates, assessment results.	5 years
Risk assessments, model validations, tuning documentation	Full working papers.	5 years, or longer under legal hold

Incoming payments with incomplete information must be identified, investigated and — where the missing information cannot be obtained from the ordering institution — escalated. Repeated failure by a correspondent to transmit complete information is a relationship-level issue for Section 9, not a payment-level exception to be repaired daily by operations.

Legal hold overrides every retention schedule. Records subject to hold must not be destroyed, archived out of reach, or migrated without Legal approval. Destruction of a record under hold is a serious disciplinary matter and may constitute obstruction.

19. Quality control, quality assurance and management information

19.1 Two distinct activities

	Quality Control (QC)	Quality Assurance (QA)
Who	Within the operating team — team leads and reviewers.	Independent QA function, reporting to the Head of Financial Crimes Operations, with a dotted line to FCC Advisory.
When	Before the decision is finalised — the four-eyes review.	After the decision is finalised — sampling of completed work.
Purpose	Prevent an error from being recorded.	Detect error rates, themes and root causes; escalate; drive training and procedure change.

	Quality Control (QC)	Quality Assurance (QA)
Coverage	100% of decisions that close risk.	Risk-based sampling. Minimum: 10% of SAR no-file decisions; 5% of alert closures; 5% of screening clearances; 10% of EDD approvals; 100% of downward risk-rating overrides; 100% of deferrals.

19.2 Error classification

Grade	Definition	Action
Critical	The error, if undetected, would result in a missed or late regulatory filing, an unreported suspicion, a sanctions breach, a tipping-off event, or an onboarding that Policy prohibits.	Immediate rework; same-day escalation to FCC Advisory; root cause within 5 business days; reported to the Financial Crimes Risk Committee; individual coaching or conduct action.
Major	A required step was omitted or performed without adequate evidence, but the outcome is not shown to be wrong.	Rework within 5 business days; trend tracked; training assigned.
Minor	Documentation, formatting or data-entry defect with no bearing on the outcome.	Corrected; tracked for theme.

19.3 Management information

Financial Crimes Operations produces a monthly operational pack — alert volumes and ageing by queue; SLA attainment; SAR volumes, timeliness and quality; screening hit and clearance rates; onboarding cycle times and deferrals; overdue periodic reviews; QA error rates by grade and theme; and open procedure deviations. The pack is submitted to the Financial Crimes Risk Committee. Metrics that are worsening must be presented as worsening; there is no re-basing of a target to make a red metric green.

Appendix A — Consolidated service-level table

Activity	Owner	Service level	Nature
Sanctions potential-match escalation	Screening Ops	2 hours	Internal (risk-critical)
Sanctions false-positive clearance	Screening Ops	Same business day	Internal
PEP match disposition	Screening Ops	2 business days	Internal
Adverse-media disposition	Screening Ops	3 business days	Internal
CIP verification	KYC Ops	Before account opening; 30 calendar days absolute	**Statutory**
Onboarding — Low / Medium risk	KYC Ops	5 business days from complete file	Internal
Onboarding — High risk / EDD	KYC Ops + FCC	15 business days from complete file	Internal
L1 alert triage	Investigations	5 business days	Internal
L2 investigation	Investigations	30 calendar days from alert	Internal
L3 case	Investigations	60 calendar days from alert	Internal
RFI response by RM	Front office	5 business days	Internal
SAR — suspect identified	Reg. Reporting	30 calendar days from initial detection	**Statutory**
SAR — no suspect identified	Reg. Reporting	60 calendar days from initial detection	**Statutory**
SAR — continuing activity	Reg. Reporting	120 calendar days from prior filing	**Statutory**
CTR	Reg. Reporting	15 calendar days from transaction	**Statutory**
314(a) response	FCC	14 calendar days	**Statutory**
§ 319(b) records production	FCC + Legal	7 calendar days	**Statutory**
OFAC blocked-property report	Sanctions	10 business days	**Statutory**
Periodic review — High	KYC Ops	12 months	Internal
Periodic review — Medium	KYC Ops	24 months	Internal
Periodic review — Low	KYC Ops	36 months	Internal

Appendix B — Alert and case disposition codes

Code	Meaning	Permitted at
FP-01	Consistent with documented KYC profile and expected activity	L1
FP-02	Explained by a verified, documented event (e.g. property sale, dividend, insurance settlement) with supporting evidence on file	L1
FP-03	Data-quality artefact; underlying activity confirmed benign; DQ defect raised	L1 (must raise a DQ ticket)
FP-04	Duplicate of an alert already investigated; prior case referenced	L1
ESC-01	Escalated — activity inconsistent with profile, unexplained	L1 → L2
ESC-02	Escalated — potential structuring	L1 → L2
ESC-03	Escalated — potential sanctions or terrorism nexus	Immediate → L3
ESC-04	Escalated — human trafficking or exploitation indicators	Immediate → L3
ESC-05	Escalated — potential insider abuse or employee involvement	Immediate → L3 and Employee Investigations
CL-01	Closed after full investigation — reasonable explanation established and documented	L2 / L3, four-eyes
CL-02	Closed after full investigation — no reasonable explanation, but no reasonable basis to suspect; rationale recorded	L3 only, with SAR Review Committee endorsement
SAR-01	SAR filed	SAR Review Committee
SAR-02	SAR filed — continuing activity	SAR Review Committee
SAR-03	SAR considered and not filed — decision and reasoning documented	SAR Review Committee; 10% QA sample
EXIT-01	Exit recommended	FCC Advisory
CIP-FAIL	Identity could not be reasonably established	KYC Ops → Investigations

Appendix C — Escalation matrix

Event	Escalate to	Within
Suspected tipping off (by any employee)	BSA/AML Officer and Legal	Immediately
Potential sanctions true match	Sanctions team	2 hours
Terrorist-financing or trafficking indicator	Senior Investigator and BSA/AML Officer	Immediately
Potential missed or late SAR	Head of Investigations and BSA/AML Officer	Same day
Account opened outside NG-KYC	Head of FC Operations	1 business day
Monitoring system outage or feed failure	Head of FC Operations and FCC Advisory	Immediately; backlog plan within 24 hours
Screening list not loaded within SLA	Head of Screening Ops and Sanctions	Immediately (OFAC: 4 hours; other lists: 24 hours)
Business pressure to alter a compliance decision	BSA/AML Officer directly, and Employee Relations	Immediately; anonymously if preferred

Event	Escalate to	Within
Employee suspected of facilitating financial crime	BSA/AML Officer, Legal, Employee Investigations	Immediately; do not investigate locally
Regulatory or law-enforcement contact of any kind	FCC and Legal	Immediately; do not respond substantively

Approval

Approved by the Global Head of Financial Crimes Compliance (designated BSA/AML Officer) on 9 April 2026, and issued by the Head of Financial Crimes Operations. Effective 1 May 2026.

— End of Procedures —