



Financial Crime Compliance Policy

Internal AML, counter-terrorist financing, proliferation financing, sanctions, fraud, bribery and tax-evasion controls for a UK SME finance brokerage.

Document control	Details
Company	Brooks Beckman Ltd Company number 12918986 ICO ZA831470
Version and status	1.0 - draft for approval; not evidence of Board adoption
Prepared	16 October 2026
Policy owner	Designated Financial Crime Lead / MLRO where appointed
Approval and review	Director / Board approval required. Review at least annually after approval and following a material change.

1. Business model and application

Brooks Beckman Ltd ("the Firm") is a credit broker, not a lender. It introduces and arranges funding including business loans, asset, property, invoice and tax finance. It does not describe itself in this policy as advancing its own loan book or administering lender repayments. Any future client-money, payment, lending or servicing activity requires a separate assessment before it begins.

This policy applies to directors, employees, contractors and associated persons acting for the Firm. It sets minimum internal standards for assessing and mitigating financial-crime risks across enquiries, applications, lender introductions, partner relationships, commission and ongoing brokerage activity. Relevant legal prohibitions take precedence over commercial objectives.

Regulatory scope - approval dependency

The directors must document the Firm's actual permissions, appointed-representative or principal arrangements, MLR scope and supervisory/registration position before adopting this policy. The policy does not assert FCA authorisation or Annex 1 registration. A broker must not inherit those claims from a lender's document, and AML registration is not equivalent to permission to conduct regulated credit or mortgage business.

Apply statutory MLR duties where the relevant activity is in scope. Where they are not directly applicable, proportionate identity, risk, escalation and screening controls remain Firm policy and may also support lender requirements. The applicability of reporting offences and supervision must be assessed by a competent person; general proceeds-of-crime, terrorism, fraud, bribery and sanctions exposure cannot be disregarded.



2. Terms, governance and accountability

Term	Meaning in this policy
AML / CTF / PF	Anti-money laundering / counter-terrorist financing / proliferation financing.
CDD / EDD / BWRA	Customer due diligence / enhanced due diligence / business-wide risk assessment.
Customer / connected party	A prospective or existing brokerage customer; relevant directors, beneficial owners, guarantors and authorised representatives.
Beneficial owner	The natural person(s) ultimately owning or controlling an entity; apply the relevant statutory test, including more than 25% ownership or voting rights and other control where applicable.
PEP / sanctions	Politically exposed person and relevant connected persons / legally binding restrictions under the applicable sanctions regime.
SAR / DAML	Suspicious activity report / a defence against specified money-laundering offences for a specified act where available; not general permission to continue a relationship.
MLRO / Financial Crime Lead	The designated lead and, where applicable, the formally appointed nominated officer, with authority and reporting routes recorded.

Directors own the framework, allocate sufficient resources, approve this policy and the BWRA and challenge material risk decisions. The lead maintains controls, training, risk assessments, registers and reports; handles suspicion escalations and liaison with relevant authorities; and has direct access to directors. Staff own first-line controls and report concerns without delay.

Confirm the named lead and trained absence cover before adoption; do not assume a CEO automatically becomes a qualified substitute. Use independent challenge proportionate to the Firm's size. An outsourced lead must have defined responsibilities, access, time and confidentiality safeguards; outsourcing does not remove directors' accountability.

Management information and training

Provide quarterly reporting and an annual financial-crime report covering risk, screening, CDD exceptions, internal and external reports, fraud, introducer issues, training and remediation. Staff must complete induction training before relevant duties and annual refreshers. Training covers role-specific red flags, escalation, sanctions, confidentiality and approved tools. Record attendance, competence checks and remedial action.



3. Risk profile and red flags

Money laundering may involve placement, layering and integration; the stages need not occur separately. Brokerage can be misused to lend credibility to false businesses, obtain finance using criminal or fabricated records, disguise ownership, arrange property or asset transactions, or redirect funds. Terrorist funding may involve legitimate sources and small amounts; PF risks may arise through connected persons, goods, jurisdictions or sanctions evasion.

Fraud exposures include false identities and documents, impersonation, manipulated invoices or tax liabilities, false property or equipment information, business email compromise, dishonest introductions and internal circumvention of controls. Verify unusual instructions independently through trusted contact details. Do not change bank or payee details solely on the strength of an email.

Bribery and corruption risks arise where gifts, benefits or referral payments influence lender or staff decisions. Do not offer, request or accept bribes, facilitation payments or concealed commissions. Record gifts and hospitality, manage conflicts and apply due diligence to introducers. The 50% partner commission arrangement must be governed by an agreement and controls; a referral payment does not justify improper influence or misleading disclosure.

VAT and Corporation Tax finance must support a legitimate liability and purpose. Do not assist false returns, fabricated liabilities, concealment or the facilitation of tax evasion. Associated-person risks fall within the Firm's prevention procedures and the Criminal Finances Act 2017 where applicable.

Examples requiring scrutiny

- Conflicting accounts, bank statements, ownership records or stated turnover; unexplained transaction patterns or beneficial ownership.
- Unusual urgency, resistance to identity checks, unexplained third-party involvement, unexpected payees or requests to conceal the source or destination of funds.
- Complex structures without a credible commercial explanation, relevant adverse information, sanctions alerts or higher-risk cross-border connections.
- Introducers repeatedly supplying inaccurate applications, asking staff to bypass controls, or seeking payments to unrelated accounts.

A red flag is a prompt to assess and escalate, not proof of criminality. Do not make unsupported allegations to customers, partners or other lenders.



4. Legal framework and scope register

The Firm has regard to the Money Laundering Regulations 2017 as amended where applicable; Part 7 of the Proceeds of Crime Act 2002; the Terrorism Act 2000; the Fraud Act 2006; the Bribery Act 2010; the Criminal Finances Act 2017; UK sanctions legislation under SAML 2018 and regime-specific regulations; and applicable data protection law.

The lead maintains an obligations register covering which activities and reporting duties apply, the authority responsible, evidence of any required registration or permission, and reporting deadlines. Use current FCA and JMLSG guidance relevant to the confirmed activity. References to rules do not establish that the Firm holds a permission or is a registered Annex 1 institution.

Principal money-laundering offences can carry up to 14 years' imprisonment. Other reporting, sanctions, terrorism and corporate offences have distinct elements and penalties. Staff must not rely on a simplified penalty table as legal advice or assume that one internal report automatically discharges every potential personal duty.

5. Business-wide and customer risk assessment

Maintain a documented BWRA considering customers and ownership, products and funding purpose, geography, transactions and commissions, non-face-to-face channels, introducers and technology. Identify inherent risk, control effectiveness and residual risk. Directors approve it annually and on material changes to products, partners, locations or threat information.

Risk-assess each customer or relationship using reliable information and record low, medium or high risk with reasons. Reassess on changes of ownership or purpose, significant adverse information, unusual instructions or screening alerts. Higher-risk cases need enhanced measures and lead/senior approval. No score can override a prohibition.

Check current geographic indicators, including applicable statutory high-risk-country requirements, FATF statements and UK sanctions. Apply the current legal test rather than hard-coding an old list or assuming every FATF category has the same statutory consequence. Record links to the customer, owners, guarantors and transaction, and keep the methodology current.

Risk appetite

Do not proceed where identity or control cannot be established to the required standard, required evidence is withheld, the purpose appears unlawful or implausible, sanctions prohibit the activity, or material risks cannot be mitigated. Escalate exceptions and reasons. The Firm's permitted customer and product scope must be approved separately; this policy does not impose another lender's incorporated-only or unsecured-only lending appetite.



6. Customer due diligence and acceptance

Identify the business and relevant individuals, verify identity using reliable independent evidence, understand ownership/control, authority to act, purpose and intended nature of the funding, and assess risk. Company-register checks support verification but are not the only evidence. Identify beneficial owners under the applicable test and address discrepancies, including any required reporting.

Sequence the process proportionately: an initial enquiry may gather limited information, but statutory or lender-required checks must be completed at the required time. Do not introduce or help complete prohibited activity, bypass a lender's checks or present incomplete checks as complete. A lender remains responsible for its own acceptance and lending decision; any reliance or delegated arrangement must be expressly documented and legally valid.

Record which party performs each check and when, including the Firm's own requirements, the lender's requirements and the basis of any permitted reliance. Use of a screening tool is not statutory third-party reliance. Where applicable MLR conditions cannot be met, do not establish or continue the relationship as prohibited and consider whether a report is needed.

Providers and non-face-to-face channels

Approve providers before use, checking data quality, sanctions-list currency, coverage, security, contracts and overseas processing. Record the provider register and annual review. The policy deliberately does not assert that any named screening platform or identity provider has been contracted by Brooks Beckman.

For remote applications, use proportionate electronic verification, authenticity checks and independent follow-up. Confirm representatives' authority and watch for impersonation, manipulated uploads and recycled identities. Keep an evidence trail of checks and decisions.

Source of funds and wealth

Understand the proposed funding purpose, deposit or contribution, expected repayment source and any unusual third-party funds to the extent relevant to the brokerage role and risk. Obtain further evidence when required by law, a lender or the risk assessment. Establish source of wealth in relevant higher-risk or PEP situations. The Firm must not claim to monitor a lender's entire repayment account where it has no such role or access.



7. Enhanced checks and politically exposed persons

Apply enhanced measures where required by current law or justified by risk, including relevant PEP relationships, higher-risk country connections, obscure ownership, unusual transactions, implausible purpose, material adverse information or inadequate remote-verification safeguards. Standard controls are not waived solely because an introducer or lender knows the customer.

Enhanced measures may include additional identity and ownership evidence, further explanation of purpose, source-of-funds/wealth evidence, closer adverse-media review, senior approval and more frequent monitoring. Record why the measures are sufficient and the decision to proceed, decline or pause.

Assess potential PEP matches rather than treating every alert as confirmed. Apply the statutory definition and proportionate risk assessment, including the applicable treatment of domestic PEPs and connected persons. Where required, obtain senior approval, establish source of wealth and funds and conduct enhanced monitoring. PEP status alone is not a criminal allegation or automatic prohibition.

8. Financial sanctions

Screen relevant customers, beneficial owners, directors, controllers, representatives and guarantors against the current UK Sanctions List and other applicable restrictions. The UK Sanctions List became the single source for UK designations following closure of the former consolidated list on 28 January 2026. Assess ownership/control and regime-specific restrictions as well as name matches; a clean name search is not a complete legal analysis.

Screen before relevant activity, at appropriate completion points and on material party or list changes. Record search inputs, date, source, result and reviewer. Document false-positive decisions. Escalate unresolved alerts immediately and hold the relevant introduction, commission payment or other transaction while the lead assesses it.

Do not deal with frozen assets or make prohibited funds or economic resources available. Where the Firm holds relevant assets, comply with the applicable freeze and reporting duties; otherwise do not imply custody. The lead determines OFSI reporting, licensing and other reporting requirements with specialist advice where needed. A DAML is not an OFSI licence and does not override sanctions prohibitions.



9. Suspicious activity and reporting

Staff must promptly report knowledge, suspicion or other relevant concerns through the confidential internal escalation route to the lead / nominated officer. Preserve records, explain the grounds and relevant parties/transactions, and do not investigate beyond the authorised task or discuss the report with the customer. The lead must be available through a documented secure route and absence arrangements.

The lead assesses all reasonably available information, considers the applicable statutory reporting tests, records whether an external report is required and why, and submits appropriate reports through current official channels. Internal reports and external SAR records are access-restricted and separated from ordinary customer notes. An internal escalation does not remove every possible legal duty of the individual; seek advice where uncertain.

DAML and other restrictions

If an intended act may engage the principal money-laundering offences, the lead obtains legal advice and, where appropriate, seeks a DAML for the specified act before proceeding. Observe the relevant statutory notice and moratorium arrangements and any extension or court restriction. Do not interpret acknowledgement of a SAR, a lack of general reply or a DAML as approval of the whole relationship.

Consider terrorist-financing, sanctions and other reporting or consent requirements separately. The lead records any permitted activity, limitations, deadlines and decision-maker. Brokerage and commission activity can need assessment even where the Firm does not advance or recover funds itself.

Tipping off and prejudicing an investigation

Do not disclose a report, suspicion or investigation where that would be unlawful or prejudice an investigation. Refer customer communications, complaint responses and data requests involving such information to the lead. Apply the specific legal test and permitted disclosures; do not make blanket claims that every customer contact about a concern is prohibited. Never include restricted suspicion records in a routine application pack or referral email.

10. Ongoing monitoring and response

Monitor activity and relationships to the extent of the Firm's role, including new introductions, ownership changes, screening events, unusual requests, changes to stated purpose and commission-payment patterns. Review higher-risk cases more frequently and at trigger events. If new information arises after referral, assess whether lawful notification to the lender or authorities is required, without prohibited disclosure.



11. Records, assurance and review

Keep evidence of identity, risk assessments, screening, approvals, introductions, relevant transactions, training, incidents and reporting decisions. Apply the Data Protection Policy and documented access controls. Where MLR Regulation 40 applies, use its five-year end-event and deletion/extension requirements. Otherwise use a justified brokerage retention schedule; do not treat every AML-labelled record as subject to the same statutory period.

The lead performs proportionate sample reviews, tests screening currency and monitors exceptions and overdue remediation. Directors receive quarterly information and commission periodic independent assurance based on risk. Findings have an owner, deadline and closure evidence. No policy exception can waive a legal prohibition; any permissible internal exception is documented, time-limited and approved at the appropriate level.

Report policy breaches immediately. Investigate, protect evidence, remediate and consider appropriate disciplinary, contractual or external action. Review the policy at least annually, and sooner following material legal changes, incidents, assurance findings or changes to the brokerage business.

Supporting records and procedures

Maintain the BWRA; customer risk methodology; due-diligence checklist and sign-off authorities; current sanctions and PEP procedures; secure internal suspicion-report route; introducer and commission controls; fraud/bribery/tax-evasion prevention records; supplier register; training log; Data Protection Policy; and Complaints Policy. These are required supporting controls, not a representation that separate documents have already been adopted.

Approval record

Before adoption, record the named lead and cover, statutory scope and supervisory status, approved customer/product scope, actual providers, escalation routes and approval date. Directors confirm implementation resources and the next review date within twelve months.



Appendix A. Monitoring plan

Activity	Frequency / owner / evidence
Induction and refresher training	Before relevant duties and annually; Lead; completion and competence records.
Onboarding file sampling	Monthly, risk-based; Lead; file-review log and corrective actions.
Higher-risk approvals and exceptions	Per case, monthly oversight; Lead / senior approver; approval and review records.
Screening quality and list currency	Monthly oversight and on material changes; Lead; test results and match decisions.
Introducer and commission controls	Onboarding and risk-based review; directors / Lead; due diligence, agreements and payment checks.
Suspicion reports and sanctions escalations	As required, without delay; Lead; restricted register and reporting decisions.
Provider and methodology review	Annually and on change; Lead; due diligence, coverage and calibration evidence.
BWRA and policy review	At least annually and on material change; directors / Lead; approval and version history.
Management information / annual report	Quarterly / annually; Lead; Board papers and actions.
Regulatory notifications and returns	Only where applicable, by confirmed deadlines; responsible officer; submission evidence.
Independent assurance	Periodic and risk-based; independent reviewer; report and remediation tracker.

Reference points checked on 16 October 2026

FCA AML registration: <https://www.fca.org.uk/firms/financial-crime/money-laundering-terrorist-financing/registration>

UK Sanctions List: <https://www.gov.uk/government/publications/the-uk-sanctions-list>

MLRs 2017: <https://www.legislation.gov.uk/ukxi/2017/692/contents>

POCA 2002: <https://www.legislation.gov.uk/ukpga/2002/29/contents>

Official SAR guidance:

<https://www.nationalcrimeagency.gov.uk/what-we-do/crime-threats/money-laundering-and-illicit-finance/suspicious-activity-reports>

This controlled internal policy should not be used as the public website AML statement without preparing an appropriate customer-facing version that excludes confidential operational arrangements.