ANTI-MONEY LAUNDERING POLICY

& COUNTER-TERRORIST FINANCING POLICY

Recovia Ltd

Document REC-POL-006 | Version 2.0 | August 2026 | Incorporated: 12 January 2026 | Owner: SMF17 MLRO

Document title	Anti-Money Laundering & Counter-Terrorist Financing Policy
Owner	SMF17 — Money Laundering Reporting Officer (MLRO)
Version	2.0 (August 2026)
Date	August 2026
Next review	June 2027 (or immediately upon legislative or regulatory change)
Approved by	Ben James Portman
Applies to	All staff, contractors and agents of Recovia Ltd

1. Policy Statement

Recovia Ltd is committed to preventing its services from being used to launder the proceeds of crime or to finance terrorism. This Policy sets out Recovia's obligations under the following legislation and guidance:

- Proceeds of Crime Act 2002 (POCA) — principal UK money laundering legislation
- Terrorism Act 2000 — counter-terrorist financing obligations
- Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs 2017, as amended)
- FCA's Financial Crime Guide (FCG)
- JMLSG Guidance — Joint Money Laundering Steering Group guidance for the financial sector

Recovia holds client money — funds recovered from debtors pass through a Recovia-administered account before remittance to clients. This creates a specific money laundering risk: the client money account could potentially be used to layer criminal proceeds. Recovia's AML controls are designed specifically to address this risk.

Breach of money laundering legislation is a serious criminal offence carrying penalties of up to 14 years' imprisonment and/or an unlimited fine. Failure to report a suspicion (a 'failure to disclose' offence) carries penalties of up to 5 years' imprisonment. All staff must read and comply with this Policy.

2. MLRO — Money Laundering Reporting Officer

Recovia's Money Laundering Reporting Officer (MLRO) is the SMF17 holder:

Name	Ben James Portman
Role	SMF17 — MLRO
Contact	contact@recoviaholdings.co.uk | 01527 369593
Responsibility	Receiving all internal Suspicious Activity Reports (SARs); assessing whether an external SAR should be filed with the NCA; maintaining AML records; annual AML review

All suspicions of money laundering or terrorist financing must be reported to the MLRO immediately. Staff must not discuss their suspicion with the person under scrutiny — this constitutes 'tipping off', which is a criminal offence under POCA s.333A.

3. Risk Assessment

Recovia has assessed its money laundering risk profile as follows:

3.1 Business-Level Risk

Nature of business	Debt recovery and claims management — not a lending or deposit-taking business. However, client money passes through Recovia's account, creating layering risk.
Client risk	Predominantly UK-based SME clients. Low risk of professional money launderers using a debt recovery service as a vehicle — but client due diligence applied nonetheless.
Debtor risk	Debtors paying debts they owe. Risk arises where: debts are paid by a third party without explanation; debts are overpaid; payments are made in cash or from unusual sources.
Geographic risk	Operations in England and Wales. International recovery undertaken via partner network — enhanced due diligence applies to international cases.
Overall ML risk rating	MEDIUM — due to client money flows through the business.

3.2 Red Flags — Indicators of Suspicious Activity

The following are specific indicators that should prompt an internal SAR to the MLRO:

- A debtor pays a debt significantly in excess of the amount owed without credible explanation
- A third party pays a debtor's debt and requests the overpayment (or the full amount) be returned to them rather than to the client
- A client instructs Recovia on a debt that appears fabricated, inflated, or not supported by genuine contractual documentation
- A debtor pays a very old or written-off debt suddenly and in full, without prior engagement
- A client or debtor requests an unusual payment method — cash, cryptocurrency, payments through multiple bank accounts
- A client or debtor requests that recovered funds be paid to a third party rather than the named creditor
- A client's ownership structure is complex, opaque or involves jurisdictions known for financial secrecy
- A new client is reluctant to provide KYC documentation without credible explanation
- Payments are received from or sent to countries on FATF high-risk jurisdiction lists

4. Customer Due Diligence (CDD)

Recovia applies Customer Due Diligence to all clients before accepting instructions. CDD is also applied to certain debtors where higher risk indicators are present.

4.1 Standard CDD — All New Clients

Before accepting a new client instruction, Recovia obtains and verifies:

Individual clients (sole traders, personal creditors):

- Full legal name
- Residential address — verified by utility bill or bank statement (within 3 months)
- Date of birth
- Photo ID — passport or driving licence (copy obtained and certified)
- Source of the debt — contractual documentation reviewed

Corporate clients (limited companies, partnerships):

- Registered company name and number — verified on Companies House
- Registered address and principal trading address
- Copy of certificate of incorporation
- Details of beneficial owners — any individual owning more than 25% of shares or voting rights (verified against PSC register on Companies House)
- Details of directors — names verified against Companies House filing
- Nature of the business — description of trading activity reviewed for plausibility
- Source of the debt — contractual documentation reviewed

4.2 Enhanced Due Diligence (EDD)

Enhanced Due Diligence is applied in addition to standard CDD in the following circumstances:

- The client is incorporated in or connected to a high-risk jurisdiction (FATF list)
- The client or any beneficial owner is a Politically Exposed Person (PEP)
- The client has complex beneficial ownership (multiple layers of corporate structure)
- The transaction or debt is unusually large or the circumstances are atypical
- The MLRO has identified a specific risk indicator requiring further investigation

EDD measures include:

- Senior management approval (SMF17/SMF1) required before onboarding the client
- Enhanced verification of source of funds and source of wealth
- More frequent monitoring of transactions during the relationship
- Detailed file notes recording the rationale for proceeding

4.3 Ongoing Monitoring

Recovia monitors all client relationships on an ongoing basis:

- Any change in the client's business, ownership structure or risk profile triggers a CDD refresh
- Unusual payment patterns by debtors are flagged to the MLRO immediately
- Clients not active for 12 months are subject to a CDD refresh before new instructions are accepted

4.4 CDD Records

All CDD documentation is retained for a minimum of 5 years from the end of the business relationship (as required by MLRs 2017 reg. 40). Records are stored securely and available for inspection by the FCA or NCA on request.

5. Suspicious Activity Reporting

5.1 Internal SAR Process

Any member of staff who suspects or has reasonable grounds to suspect that money laundering or terrorist financing is occurring or has occurred must:

1. Report their suspicion to the MLRO immediately using the Internal SAR Form (Appendix A)
2. NOT discuss the suspicion with the client, debtor or any other party — this constitutes tipping off
3. NOT take any further action on the relevant case until the MLRO has assessed the SAR
4. Retain all documents and records relating to the suspicion

5.2 MLRO Assessment

Upon receipt of an internal SAR, the MLRO will:

5. Acknowledge receipt to the reporting staff member within 1 business day
6. Assess the SAR against available information — reviewing the case file, client CDD, transaction records and any other relevant material
7. Decide within 5 business days whether to file an external SAR with the NCA or to take no further action
8. Record the decision and rationale on the SAR log (Appendix B)

Where the MLRO decides to file an external SAR:

- The SAR is submitted via the NCA's SARs Online system at www.nationalcrimeagency.gov.uk
- Where a transaction is involved, a Defence Against Money Laundering (DAML) consent request is made to the NCA before proceeding with the transaction
- Recovia does not proceed with the transaction until NCA consent is obtained or the 7-day moratorium period expires

5.3 Tipping Off

It is a criminal offence under POCA s.333A to disclose to a client or debtor that a SAR has been filed or that an investigation is being conducted. Staff must not, under any circumstances, indicate to any party that a SAR has been made or is being considered. If in doubt, speak only to the MLRO.

6. Sanctions Screening

Before accepting a new client or debtor instruction, Recovia screens against:

- HM Treasury financial sanctions list (UK Sanctions List) — www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets
- OFAC SDN list (where US persons or US-dollar transactions are involved)
- UN Security Council consolidated sanctions list

Screening is performed at onboarding and repeated annually for active clients. Any match or potential match is reported to the MLRO immediately and no funds are transferred until the match has been assessed and cleared or the relevant authority has been notified.

7. Training

All staff receive AML training:

- On joining Recovia — before handling any client money or taking instructions
- Annually — refresher training covering any legislative or regulatory developments
- Immediately — upon any material change to this Policy or AML legislation

Training records are maintained by the MLRO and available for FCA inspection. Training covers: what money laundering is and how it works; Recovia's specific ML risk profile; how to identify red flags; how to report to the MLRO; what tipping off is and why it is a criminal offence.

8. Record Keeping

CDD records	5 years from end of the business relationship (MLRs 2017 reg. 40)
Transaction records	5 years from the date of the transaction
Internal SAR records	5 years from date of submission
External SAR records	5 years from date of submission to NCA
Training records	5 years from date of training

9. Annual AML Review

The MLRO conducts an annual review of Recovia's AML controls, which includes:

- Review of all internal SARs filed during the year
- Assessment of whether any systemic risk indicators were missed
- Review of any regulatory or legislative changes affecting Recovia's obligations
- Update of this Policy where required
- Review and update of staff training materials
- Sign-off by SMF1 and retention on file

Appendix A — Internal SAR Form

Date of report	
Reporting staff member	
Client / case ref	
Nature of suspicion	
Specific transaction / event that prompted the report	
Any documents attached	
Date reported to MLRO	
MLRO receipt confirmed	

Appendix B — SAR Log

SAR Ref	Date received	Source	Nature	MLRO decision	Date of decision	NCA ref (if filed)