

1. PURPOSE

The purpose of this policy is to prevent Impact Financial Services Limited from being used for money laundering, terrorist financing or other financial crime.

This policy sets out the systems, controls and procedures required to comply with:

- the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (as amended),
- the Proceeds of Crime Act 2002,
- the Terrorism Act 2000,
- the FCA Handbook and Financial Crime Guide,
- JMLSG Guidance.

2. SCOPE

This policy applies to all:

- directors,
- advisers,
- employees,
- appointed representatives,
- contractors

of Impact Financial Services Limited.

3. REGULATORY STATUS AND RESPONSIBILITY

Impact Financial Services Limited is authorised and regulated by the Financial Conduct Authority (FCA).

Firm Reference Number (FRN): **1025644**.

Money Laundering Reporting Officer (MLRO)

The firm has appointed a Money Laundering Reporting Officer (MLRO), also referred to as the Nominated Officer (NO).

MLRO / Nominated Officer: Jakub A. Madejewski

The MLRO has overall responsibility for:

- overseeing AML controls,
- receiving internal suspicious activity reports,
- deciding whether to submit SARs to the NCA,
- maintaining AML records and policies.

4. RISK-BASED APPROACH

The firm operates a risk-based approach to AML and CTF.

Risk assessments consider:

- customer risk,
- geographic risk,
- product and service risk,
- delivery channel risk.

Enhanced controls are applied where higher risk is identified.

5. CUSTOMER DUE DILIGENCE (CDD)

CDD must be completed:

- before entering into a business relationship,
- before carrying out a transaction,
- when there is doubt about previously obtained identification,
- when there is suspicion of money laundering or terrorist financing.

CDD includes:

- verification of identity,
- verification of address,
- understanding the purpose and nature of the business relationship,
- source of funds and source of wealth where appropriate.

6. ENHANCED DUE DILIGENCE (EDD)

Enhanced due diligence is required for higher-risk situations, including:

- Politically Exposed Persons (PEPs),
- clients from high-risk jurisdictions,
- complex or unusual transactions.

EDD may include:

- additional identity checks,
- senior management approval,
- enhanced ongoing monitoring.

7. POLITICALLY EXPOSED PERSONS (PEPs)

The firm identifies and manages PEP relationships in accordance with MLR 2017.

Where a PEP relationship is identified:

- enhanced due diligence will be applied,
- approval from senior management is required,
- ongoing monitoring will be conducted.

8. ONGOING MONITORING

All client relationships are subject to ongoing monitoring to ensure that:

- transactions are consistent with the firm's knowledge of the client,
- documentation remains up to date,
- any unusual activity is identified promptly.

9. SANCTIONS SCREENING

The firm screens clients against:

- UK sanctions lists,
- international sanctions regimes where appropriate.

Any positive match must be escalated immediately to the MLRO.

10. SUSPICIOUS ACTIVITY REPORTS (SAR)

All staff must report any knowledge or suspicion of money laundering or terrorist financing to the MLRO without delay.

The MLRO will assess whether a Suspicious Activity Report (SAR) must be submitted to the National Crime Agency (NCA).

Tipping-off

Staff must not disclose to a client or any third party that:

- a SAR has been made, or
- a SAR is being considered.

This includes any action that could constitute tipping-off.

11. PAYMENT METHODS

The firm operates strict payment controls.

Cash payments are not accepted under any circumstances.

All payments must originate from an account held in the client's own name, unless expressly approved by the MLRO.

Third-party payments are not permitted without enhanced checks and MLRO approval.

12. INTRODUCERS AND THIRD PARTIES

All introducers must be approved by Compliance before any business is accepted.

The firm conducts:

- initial due diligence on introducers,
- ongoing monitoring and periodic review to ensure continued compliance.

The firm remains responsible for AML compliance on all introduced business.

13. RECORD KEEPING

AML records will be retained for:

- a minimum of five years after the end of the business relationship, or

- longer where required by law or regulation.

Records include:

- CDD/EDD documentation,
- risk assessments,
- SAR decisions,
- training records.

14. TRAINING AND AWARENESS

All relevant staff must receive AML training:

- at induction,
- on an ongoing basis.

Training covers:

- AML legislation,
- identifying suspicious activity,
- internal reporting procedures,
- consequences of non-compliance.

15. BREACHES AND ESCALATION

Any breaches of this policy must be reported to the MLRO and managed in line with the firm's Compliance Breach & Disciplinary Policy.

Serious breaches may result in:

- disciplinary action,
- termination,
- regulatory reporting where required.

16. REVIEW OF THIS POLICY

This policy will be reviewed:

- at least annually,
- following regulatory change,
- or following material AML incidents.

Policy Review and Approval:

This policy will be reviewed annually or more frequently if required by changes in regulations or the needs of the firm. All amendments will be documented and communicated to all staff members.