Financial crime policy

2021

A. Context

1. Introduction

Financial crime risks expose firms to the potential for serious reputational damage, regulatory censure and financial loss and may cause detriment or loss to clients. No firm can consider itself to be immune from the possibility of being used to further financial crime. We take financial crime risks very seriously, and have robust financial crime risk management arrangements. Financial crime includes wrong-doing such as internal and external fraud, money laundering and terrorist financing. Further definitions are included under Scope and Definitions below.

We are required to comply with relevant legislation including the Proceeds of Crime Act 2002, as amended by the Serious Organised Crime and Police Act 2005 and the Serious Crime Act 2015, the Terrorism Act 2000, the Money Laundering Regulations 2007, and relevant FCA requirements set out in SYSC 3.2.6 and 6.1. In this policy, we refer to anti-money laundering and countering terrorist financing as AML/CTF and associated risks as ML/TF risks.

The Firm is also subject to certain anti-money laundering obligations under U.S. law, most of which are covered by this policy.

2. Scope & definitions

In this policy, the term *'staff'* includes directors and employees as well as temporary staff such as contractors and consultants, all of whom are covered by this policy.

This policy sets out arrangements in respect of Lendable clients, i.e. SPCs, Funds and segregated accounts managed by Lendable.

The Financial Services and Markets Act 2000 defines ***financial crime*** to include any offence involving:

(a) Fraud or dishonesty;

(b) Misconduct in, or misuse of information relating to, a financial market; or

(c) Handling the proceeds of crime.

The use of the term 'to include' means financial crime can be interpreted widely to include, for example, corruption or funding terrorism. This policy focuses particularly on (a) and (c) and includes anti-money laundering and countering terrorist financing. Separate policies are in place

covering Anti-Bribery and Corruption and Market Abuse. The Criminal Finances Act has broadened the definition of financial crime to also include facilitation of tax evasion which may lead to criminal charges, sanctions and/or reputational damage.

Money laundering is the process by which the proceeds of crime are converted into assets which appear to have a legitimate origin. There are three principal money laundering offences under the Proceeds of Crime Act ("POCA") i.e. behaviour that directly constitutes money laundering. These are "concealing", "making arrangements" and the "acquisition, use and possession" of criminal property.

3. Risk appetite

Lendable has no tolerance for being used as a vehicle for financial crime.

Any breach of this policy will be treated as an extremely serious matter and is likely to result in disciplinary action.

B. POLICY APPLICATION & MANAGEMENT

1. Roles & responsibilities

Staff must:

- Be aware of financial crime risks and potential sources of financial crime, and your obligations in relation to those risks and associated controls.
- Immediately on detection, report any suspicious transaction or activity to the MLRO. However, you must not alert/tip off any of the people concerned to your suspicion.
- Complete annual AML training in accordance with the compliance training programme set for you.
- Assist in any investigation into any suspected instance of financial crime.

The MLRO is responsible for:

- Receiving suspicious transaction reports/disclosures, determining whether or not these give rise to knowledge or suspicion of money laundering or reasonable grounds for knowledge or suspicion and, where this exists, making a report to the National Crime Agency ("NCA").
- Ensuring that financial crime risks have been appropriately assessed, and that effective controls are in place to mitigate these risks.
- Providing oversight over the risk-based approach to prevention of money laundering/terrorist financing.
- Ensuring that staff receive suitable AML/CTF/financial crime prevention training, and that appropriate training records are kept.

- At least annually, making a report to the firm's governing body on the operation and effectiveness of the firm's systems and controls for detecting and preventing financial crime.

The Directors are responsible for:

- Periodically (at least annually) reviewing reporting from the MLRO on the effectiveness of systems and controls in place to detect and prevent financial crime.
- Ensuring that the MLRO has sufficient independence and resources to discharge the responsibilities of a CF11.

2. Policy application

2.1 Money Laundering Reporting Officer

Lendable has appointed a Money Laundering Reporting Officer ("MLRO") who has been approved by the FCA to hold Controlled Function 11.

The Money Laundering Reporting Officer is the Chief Operating Officer, Des Denning. Any suspicions or concerns should be raised with the MLRO. In his absence, or in any instance where it is suspected that the MLRO is involved in the suspicious transaction(s), concerns should be raised with the Chief Operating Officer.

2.2 Risk-based approach to Financial Crime Prevention

Financial crime risks and associated controls are identified on the Lendable risk register. These risks are reviewed regularly (at least six monthly) by the MLRO. In addition, the MLRO makes an assessment of the overall risk of the business being used as a vehicle for financial crime. This assessment is based on the following risk factors:

- Clients
- Products and services
- Distribution channels
- Geographies
- Other qualitative factors

Given the nature of the client base, SMEs and MSMEs in Emerging Markets, the risk of money laundering and other financial crime is assessed as high.

2.3 Staff recruitment, vetting and training

When recruiting new staff or promoting staff into roles that poses a higher financial crime risk, we must be satisfied as to their competence and fitness and probity.

All staff members are required to successfully complete regular AML training. This training also covers tax evasion.

Staff vetting needs to be appropriate to the role to be undertaken and the associated risks. Identification and basic criminal records checks are carried out in respect of all new recruits

including contractors. Those joining as partners and/or undertaking Approved Persons roles are also subject to credit checks. Additional checks may be undertaken if a staff member is undertaking higher-risk roles such as those involving the ability to authorise payments.

2.4 Customer Due Diligence (Investors in Funds, SMAs or SPCs)

All new clients must be subject to customer due diligence ("CDD") before monies/in specie transfers are received. Firstly, an assessment of the AML/CTF risks posed by the investor will be conducted. The key risk factors to be considered are:

- the investor type and structure;
- the geographical location of the investor;
- the regulatory status of the investor;
- distribution channel

Based on this risk assessment, the investor will be assigned to one of the following CDD categories:

- Standard customer due diligence ("SDD")
- Enhanced customer due diligence ("EDD")

The CDD category assigned will determine the nature and level of documents and information needed to complete verification process.

Arrangements for CDD

CDD is carried out for us by our Administrators, Centaur/TMF. A service level agreement is in place between Lendable and Centaur/TMF in respect of these arrangements. Centaur/TMF has AML/CTF policies and procedures which set out the risk-based approach followed. This includes the risk rating model used to assess ML/TF risks posed by investors and the documentation to be provided by investors based on the CDD category assigned and the investor type. Centaur/TMF staff is required to undertake regular AML/CTF training. The MLRO will seek confirmation and evidence of these arrangements.

Centaur/TMF requests documents for each investor, tracks details of outstanding documents and the dates of requests made for any non-AML compliant investors and retains the documents. Centaur/TMF will carry out such investigations as are necessary in order to ensure compliance with AML legislation and requirements. This will include, where relevant, verification of the identity of beneficial owners of the client and any known Politically Exposed Persons (see below) affiliated with the client. Centaur/TMF's investigations will also include relevant Financial Sanctions checks.

The Lendable MLRO will liaise with Centaur/TMF throughout this process and may assist Centaur/TMF in obtaining documents from the client where necessary and passing these on to Centaur/TMF. In the case of segregated accounts, once Centaur/TMF have received all necessary documents and satisfactorily completed CDD, they will provide a letter of comfort and any other information required to enable Lendable to comply with AML legislation. However, for the

purposes of the client take-on process, it will be sufficient to have received email confirmation from Centaur/TMF that CDD has been successfully completed.

Reliance on third parties

When undertaking CDD, Centaur/TMF and Lendable may place reliance on third parties where this is in accordance with Regulation 17 of the Money Laundering Regulations and related guidance such as that provided by the Joint Money Laundering Steering Group. In such cases, Centaur/TMF will obtain a Letter of Undertaking from the Relevant Third Party confirming that it meets the relevant requirements.

Name Screening

Centaur/TMF will screen the investor name, and any related party names (directors, beneficial owners, authorised signatories) to determine any potential connections with negative news, sanctioned countries, entities, or individuals, or politically exposed persons. Screening is carried out using World-Check which correlates most known sanction and embargo lists from around the world, including those of OFAC, UK HMT, EU, OSFI, FATF and the Australian DFAT.

All investors, associated parties and directors, where applicable, are screened against World-Check on a period basis thereafter

Potential matches are reviewed and the outcome is documented and recorded by Centaur/TMF. Following a review, where the potential match is determined to be a false positive, no further action is required. Where a potential match is confirmed as a positive match then this is escalated to the Centaur/TMF and Lendable MLROs to determine the appropriate action.

Sanctions and Asset Freezing

We are required to comply with a range of financial sanctions, particularly those imposed by UK HMT, OFAC, EU and the UN.

In the event that an investor is matched to a terrorist list, the investor account will be frozen and/or the transaction stopped and the match reported by the applicable MLRO to the relevant UK, Luxembourg or Cayman authority. No service or transaction in respect of the account will be carried out until the reports have been made.

For fund and client investments, sanctions have also been imposed by the EU, OFAC and national regulators on debt and equity issues.

Politically Exposed Persons ("PEP")

A PEP is a person who is, or was in the preceding year, entrusted with a prominent public function, or an immediate family member, or known close associate of a PEP. A PEP generally presents a higher risk for potential involvement in bribery and corruption by virtue of their position and the influence that they may hold. Once a PEP the investor will continue to be treated as a PEP.

Where an investor or beneficial owner has been identified as a PEP, either through automated screening, or self-declaration, Centaur/TMF will apply EDD. This involves, in addition to standard CDD, identification requirements, and obtaining the following additional items prior to subscription:

- Additional proof of residential address, for individuals;
- Source of wealth declaration, for individuals;
- Source of wealth confirmation (from audited financial statements) for entities;
- The approval of one of the Directors.

Note that verification checks will sometimes identify board directors of clients as being PEPs. For example, where board directors of state-owned pension funds are government officials. However, unless these individuals are beneficial owners, or where other money laundering or terrorist financing risks are present, it will normally be appropriate to apply SDD.

Centaur/TMF reviews the status of previously identified PEPs on a regular basis but, for the reasons given above, would not normally extend this to directors of entities that are deemed to be low risk.

Where an existing investor or beneficial owner has been identified as a PEP during the course of name screening, ongoing monitoring, or as a result of self-declaration the account will be treated as non-AML compliant until such time as the above EDD requirements have been obtained-refer to section "Oversight of Outstanding CDD" for further details.

Ongoing Monitoring and Refresh of CDD

In order to ensure that investor AML/CTF risk assessments remain up to date and information held on investors and clients is current and adequate Centaur/TMF employs a process of ongoing monitoring. This involves a combination of trigger led events and ad hoc and periodic reviews of the AML/CFT risk assessment, name screening on a weekly basis, and requests for additional or updated documents or information where that on file is determined to be inadequate. The frequency of periodic reviews is determined by the AML/CTF risk of the investor. The Lendable MLRO may ask Centaur/TMF to undertake a review of an investor's AML/CTF risk assessment and CDD requirements where the MLRO becomes aware that a trigger event has occurred. Trigger events are changes in the investor's status such as a change of name, shareholding, director, etc.

Where an investor's AML/CFT risk is determined to have increased, the MLRO will contact the investor to request the required additional documentation and information which corresponds to the updated risk category. The investor account will be treated as non-AML compliant until such time as the additional requirements have been satisfied - refer to below section on Oversight of Outstanding CDD for further details.

Minimum CDD Documentation

The Fund Administrator, Centaur/TMF, carries out CDD on all new investors prior to establishing a business relationship (prior to the account opening). In order to identify the investor and beneficial owner (where applicable), Centaur/TMF requires the following information:

- Name and address of the investor;
- Names(s) of the beneficial owner(s);
- Account name in respect of which monies or in specie transfers will be remitted.

This is the minimum that Centaur/TMF requires where there is reduced risk of financial crime, however their general policy is to only set up accounts once all documentation in copy format has been received.

Oversight of Outstanding CDD

As noted in section 2.4 above, CDD must be completed before monies/portfolios are transferred by/to a client. If updated documentation is required at a later date, for example due to a trigger event, the MLRO will follow up with the client to obtain the documentation.

In the event that the client fails to provide the appropriate verification documentation, the Centaur/TMF MLRO will refer this to the Directors who will decide what action to take including whether the business relationship is to be discontinued. It will not normally be appropriate to accept further monies from a non-AML compliant investor until such time as the requested documents have been received and checks completed.

Contact with the investor at each interval and receipt of any item of outstanding CDD is documented by Centaur/TMF who will provide monthly reports to the Directors on any non-AML compliant investors.

Where an investor has failed to provide the required CDD documents following a series of requests, Centaur/TMF and Lendable will need to consider whether to file a report with the regulators. This decision will be based on the available information and an assessment of the possibility of the investor being involved in money laundering or terrorist financing.

Identification, evaluation and reporting of suspicious transactions or activities

The NCA analyses SARs and uses them to identify the proceeds of crime. It counters money laundering and terrorism by passing on important information to law enforcement agencies so they can take action.

The MLRO's evaluation record should include:

- A documented outline of the research that the MLRO has undertaken into the transaction and the information that is held in relation to the customer;
- A list of any documents examined during the enquiry (which should also be retained with this record);
- What conclusions she/he has drawn from his or her findings;
- What decisions she/he has reached as regards to whether or not to disclose and how his/her conclusions have led to that decision;
- The date and time of the final completion of the record; the record should then be signed by the MLRO.

This record and supporting documentation must be retained securely.

The MLRO's decision on whether or not to submit a report to the NCA will be final and must not be subject to the consent or approval of other members of management. The MLRO may choose to notify the person who made the report of his/her decision on whether to submit a SAR to the

NCA.

Where the MLRO suspects money laundering or terrorist financing, it will normally be necessary to suspend the transaction unless it is impractical or unsafe to do so. The MLRO will provide guidance on whether processing of transactions may recommence.

2.5 *Customer Due Diligence (Borrowers that funds are disbursed to)*

The procedures for CDD on borrowers broadly follow the same procedures detailed in section 2.4 however Lendable in the case of the borrowers performs the actual CDD

For any new borrower the following information is required:

For Companies:

- Certificate of Incorporation
- Memorandum & Articles
- Most recent Audited Financial Statements
- Certificate of Shareholders

For Individuals (Includes Principals & > 10% Shareholders)

- Copy of valid passport
- Proof of address (within 3 months)
- World check background checks

In addition for individuals further background checks such as credit, criminal and reputational checks may be carried out by appointed third party agents.

No Tipping off

Where information in relation to a potentially suspicious transaction is obtained, neither Lendable nor Centaur/TMF must make any disclosure that is likely to prejudice an investigation that may be contemplated and/or conducted following the making of a suspicious activity report.

Record Keeping

Training, vetting, evaluations and reporting required by this policy and any associated investigations and reports will be retained for a minimum of five years. These records may be retained in electronic form and/or relocated to secure offsite storage provided that they are readily accessible within a reasonable time frame.

3. Measures of effectiveness, monitoring and reporting

The MLRO is responsible for monitoring compliance with this policy, and will report on issues and findings to the relevant governance forum as explained in section B1 above.

The MLRO will conduct an annual site visit to Centaur/TMF to review the AML/CFT arrangements in place to ensure compliance.

This will normally include sample testing of the AML checks they have undertaken on investors and to review other arrangements in place within Centaur/TMF to ensure compliance with applicable money laundering legislation. Any findings from this review will be reported to the Directors and actions taken as appropriate. Currently Investors in the Leaf Structures are deemed a very low risk so sample checks can be requested and tested remotely on an annual basis.

As noted earlier, Centaur/TMF is responsible for undertaking all relevant AML checks on the investors in the Fund. However, in our capacity as managers of the Fund, Lendable will monitor the arrangements that Centaur/TMF has in place to comply with applicable money laundering and anti-financial crime legislation through the annual site visit to Centaur/TMF and through review of quarterly reports from Centaur/TMF detailing compliance with applicable money laundering legislation.

The MLRO will conduct an annual review of financial crime risk management and systems and controls, and will report to the Directors on the adequacy and effectiveness of these arrangements.

The MLRO will complete the Annual Financial Crime Report to be submitted to the FCA in accordance with FCA SUP 16.23. This report is required to be completed and submitted within 60 days of the end of Lendable's financial year, i.e. by end-May each year.

4. Breach reporting

Any breaches or suspected breaches of this policy must be reported immediately to the MLRO.