Contents

4 FINANCIAL CRIME

4.1 Introduction

SYSC 6.1.1 R requires the Firm to implement and maintain adequate policies and procedures for countering the risk that the Firm might be used to further financial crime.

As an authorised principal to a number of ARs, the Firm is also responsible for supervising its ARs' compliance with relevant financial crime requirements by monitoring and enforcing compliance with the financial crime policies and procedures contained within the Manual.

Financial crime is defined under FSMA to include any offence involving:

- Fraud or dishonesty.
- Misconduct in, or misuse of information relating to, a financial market.
- Handling the proceeds of crime.
- The financing of terrorism.

The FCA's Financial Crime Guide contains practical assistance and information for firms of all sizes and across all FCA supervised sectors on actions they can take to counter the risk that they might be used to further financial crime, generally and in relation to specific risks, such as fraud and money laundering.

4.1.1 Awareness of and Training of Staff

Appropriate training will be provided to all members of Firm staff, Approved Persons and relevant AR employees/staff members as notified by the AR to the Firm, in relation to anti-money laundering in accordance with SYSC 6.3.7 G. The training forms part of the induction process for new joiners and part of the onboarding process for ARs and is repeated at least once every 12 months for all Approved Persons and relevant staff of the Firm. The MLRO is responsible for updating, or arranging the updating of, the financial crime training and it is the MLRO who should be contacted with any questions in this regard. However, annual review of financial crime training forms part of the annual review of all online training modules, which is arranged by the Compliance Officer. The compliance team, under the supervision of the Compliance Officer, keeps a record of the date the training was given, the nature of training, names of staff who received the training and results of tests undertaken by staff, where appropriate.

4.1.2 MLRO and Other Arrangements

SYSC 6.3.8 R requires that the Firm allocate to a partner or senior manager (who can also be the MLRO) overall responsibility within the Firm for establishing and maintaining effective money laundering systems and controls. This responsibility (and the corresponding Prescribed Responsibility (d) under the SM&CR) has been allocated to Kevin Gallacher.

SYSC 6.3.9 R requires the Firm to appoint an individual as the Firm's MLRO with responsibility for oversight of the Firm's compliance with the FCA's rules on systems and controls against money laundering. Senior management must ensure the MLRO has sufficient seniority and has access to resources and information to carry out the role. The FCA expects the Firm's MLRO will be based in the UK and must be an FCA Approved Person.

Under Regulation 21(3) of the Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations (as amended) (the MLRs 2017), the Firm is required to name a Nominated Officer to receive and review internal disclosures (suspicious activity reports or SARs) under Part 7 of the Proceeds and Crime Act 2000 (POCA) and the Terrorism Act 2000 (TA).

Emma Jones is the Firm's MLRO and Nominated Officer with both roles being collectively referred to as the MLRO role in this Manual. She has been approved by the FCA to undertake SMF 17 – MLRO function, and acts as the focal point for the oversight of all activity relating to anti-money laundering. She can pass on issues to the National Crime Agency (NCA) and request a defence to a money laundering offence, as appropriate. The MLRO is able to monitor day-to-day operations of anti-money laundering policies within the Firm and is able to respond promptly to any reasonable request for information made by the NCA, FCA or another enforcement body.

Queries from ARs relating to the Firm's financial crime policies and procedures should be directed to their Primary Contacts in the first instance. Submission of suspicious activity reports (SARs) should be sent *directly and confidentially* to the MLRO/Deputy MLRO, as outlined in the relevant section below.

In the MLROs absence queries should be directed to the Deputy MLRO, Gillian Gallacher. If the position of MLRO falls vacant, a replacement will be appointed by the management Governing Body and registered as an Approved Person for SMF 17 with the FCA.

The **MLRO's responsibilities** include:

1. Receiving internal reports of suspected money laundering from within the Firm.
2. Reporting to NCA.
3. Obtaining and using national and international findings.
4. Overseeing adequate arrangements within the Firm for money laundering awareness and training in line with current legal and regulatory requirements.
5. Maintaining anti-money laundering record-keeping arrangements.
6. Making annual reports to senior management about money laundering compliance in respect of criminal property, money laundering and terrorist financing risks.
7. Ensuring that money laundering risk is taken into account in the Firm's day-to-day operations, e.g. development of new products, taking on of new customers and changes in business profile.
8. Ensuring appropriate documentation of risk management policies and risk profile in relation to money laundering, including documentation of its application of those policies.

4.1.3 Record-Keeping

Copies of client identification evidence must be retained for a minimum of 5 years from the end of the relationship with the client. Transaction records must be retained for 5 years from the end of the business relationship or after the date of an occasional transaction. Notwithstanding this, it is the intention of the Firm to retain ALL records for a minimum of 5 years. Training records should include when anti-money laundering training was given.

Upon the expiry of the 5-year period the Firm must delete any personal data unless either:

- The Firm is required to retain records containing personal data by, or under, any enactment, or for the purposes of any court proceedings.
- The data subject has given express consent to the retention of that data.

Although a regulatory or legislative requirement can override a data subject's rights, information need not be kept beyond 10 years for any transaction during a business relationship even if the business relationship has not ended.

4.2 Market Conduct

Both insider dealing and market manipulation meet the FSMA definition of financial crime. In December 2018, the FCA updated its Financial Crime Guide (FCG) and the FCG now includes a chapter on insider dealing and market manipulation – FCG 8.

4.2.1 Insider Dealing

Insider dealing is made a criminal offence in Part V, section 52 of the Criminal Justice Act 1993 (CJA). The CJA makes it an offence to use non-public price-sensitive information (inside information) in order to make a profit or avoid a loss when dealing in securities, derivatives or other investments ('securities') or to enable anyone else to do so. It is also possible for a transaction which involves insider dealing to constitute a breach of the Law and incur penalties otherwise than under the insider dealing provisions of the CJA.

Importantly, under insider dealing legislation, potential liability can continue for at least as long as the information is not made public, so staff members' responsibilities may not cease upon leaving the Firm.

4.2.2 Market Manipulation

Under sections 89-91 of the Financial Services Act 2012, certain behaviours (collectively referred to as 'market manipulation') amount to criminal offences:

- Misleading statements – making false or misleading statements, promises or forecasts, dishonestly conceals or withhold any material facts.
- Misleading impressions – any action or course of conduct that creates a false or misleading impression of the market. This could include giving advice recklessly.
- Misleading statements or impressions in relation to benchmarks.

The penalty on conviction of a criminal offence of insider dealing or market manipulation can be up to 10 years' imprisonment and an unlimited fine. Furthermore, under common law a client may sue the Firm for damages. It should be noted that most legal actions under these sections of FSMA are likely to be taken against staff members of firms rather than firms themselves.

4.3 Market Abuse

The EU's Market Abuse Regulation (EU MAR) came into effect on 3 July 2016 and was onshored through the Market Abuse (Amendment) (EU Exit) Regulations to create the UK's Market Abuse Regulation (UK MAR). Changes were made to EU MAR to reflect the UK's new position outside the EU and to ensure UK MAR operates effectively in the UK. Changes were also made to ensure the UK's overseas territories are within the scope of EU MAR. However, the policy approach of EU MAR was not altered through onshoring. Therefore, in practical terms firms should not experience significant changes under UK MAR.

UK MAR contains the following legislation, technical standards and guidance:

- EU Market Abuse Regulation as amended by the Market Abuse Exit Regulations 2019 (therefore, the 2 sets of regulations need to be read together).
- FCA Technical Standards relating to UK MAR.
- ESMA Guidelines and ESMA questions and answers that existed before the end of the transition period.
- FCA guidance: FCA Handbook.

UK MAR aims to increase market integrity and investor protection, enhancing the attractiveness of securities markets for capital raising. It contains prohibitions of insider dealing, unlawful disclosure of inside information and market manipulation, and provisions to prevent and detect these.

The FCA's webpage on the Market Abuse Regulation aims to assist readers of the FCA's Handbook and contains links to relevant information sources.

MAR 1 of the FCA's Handbook MAR sourcebook provides assistance in determining whether or not behaviour amounts to market abuse. However, it should be noted that the chapter does not exhaustively describe all types of behaviours that may indicate market abuse.

Six types of behaviour (market conduct) are defined as market abuse by the Market Abuse Regulation:

1. Insider dealing (Handbook reference: MAR 1.3).
2. Unlawful disclosure (Handbook reference: MAR 1.4).
3. Manipulating, or attempting to manipulate, transactions (Handbook reference: MAR 1.6).
4. Manipulating devices (Handbook reference: MAR 1.7).
5. Dissemination (of false or misleading information) (Handbook reference: MAR 1.8).
6. Misleading behaviour and market distortion (Handbook reference: MAR 1.9).

The above headings are elaborated on below. Full descriptions/explanations and links to relevant articles of the regulation are available in the MAR sourcebook of the FCA's Handbook. The scope of investments covered by the regime is also detailed and this can include, in some cases, indices not just qualifying securities.

It is an offence to carry out any activity that amounts to market abuse.

4.3.1 Insider Dealing

Insider dealing is dealing, or attempting to deal, on the basis of inside information. Inside information is defined under Article 7 of UK MAR as information that:

- Is precise in nature.
- Has not been made public.
- Relates, directly or indirectly, to one or more issuers or financial instruments.
- If made public, would likely have a significant effect on the prices of those, or related derivative, financial instruments.

Information would be considered 'precise' if it indicates a set of circumstances which exists or may reasonably be expected to come into existence, or an event which occurred or may reasonably be expected to occur, specific enough to conclude as to its possible effect on the prices of the financial instruments or related derivative financial instrument (Article 7.2).

UK MAR also clarifies that using inside information to amend or cancel an order shall be considered insider dealing.

Examples of insider dealing include front running/pre-positioning; dealing or attempting to deal whilst in possession of inside information concerning a proposed takeover bid.

4.3.2 Unlawful Disclosure

Unlawful Disclosure refers to disclosing information relating to qualifying investments other than in the proper course of professional duties.

UK MAR has clarified that recommending or inducing another person to transact on the basis of inside information also amounts to unlawful disclosure of inside information.

Examples include: selective briefing of analysts; selective/unprofessional disclosure of information by the directors of an issuer.

4.3.3 Manipulating, or Attempting to Manipulate, Transactions

Manipulating, or attempting to manipulate, transactions refers to trading activity that could create a misleading impression as to the supply of, demand for, or price of qualifying investments.

Examples include: buying or selling at the close of the market with the effect of misleading investors who act on the basis of closing prices; sale or purchase where there is no change in beneficial ownership effected with the intention of misleading investors; entering orders into an electronic trading system and withdrawing them before they are executed with the intention of misleading investors; abusive squeezes.

4.3.4 Manipulating Devices

Manipulating devices refers to employing fictitious devices or any other form of deception with regard to a qualifying investment.

Examples include: voicing an opinion about a qualifying investment whilst holding a position in the investment and profiting subsequently from the effect of the market acting on that opinion; a series of transactions that are designed to conceal the ownership of a qualifying investment so that disclosure requirements are circumvented by the holding of the qualifying investment in the name of a colluding party, such that disclosures are misleading in respect of the true underlying holding.

4.3.5 Dissemination (of False or Misleading Information)

Dissemination (of false or misleading information) is the distribution of information which gives a false or misleading impression as to a qualifying investment. Dissemination of misleading information or unsubstantiated rumour is regarded as market abuse (see the Firm's policy at Appendix I).

4.3.6 Misleading Behaviour and Market Distortion

Misleading behaviour and market distortion refer to actions (e.g. physical movement of commodity stocks) that could create a misleading impression as to the supply of, demand for, or price of a qualifying investment.

4.3.7 Examples of Market Abuse

Please refer to Appendix H for specific examples of what may or may not constitute market abuse.

4.3.8 Suspicious Transaction and Order Reports (STORs)

Under UK MAR, firms that professionally arrange or execute transactions in certain financial instruments (as specified in Article 4 of UK MAR), and operators of UK trading venues, must report suspicious transactions and orders (STORs), or suspicions of attempted market abuse, to the FCA without delay through the Connect system using the STOR form. For further information on reporting suspected market abuse to the FCA, visit the FCA's dedicated webpage.

A suspicious transaction or order is one where there are 'reasonable grounds' to suspect it might constitute market abuse, such as insider dealing or market manipulation.

Staff members should decide on a case-by-case basis whether there are reasonable grounds for suspicion, taking into account the deciding circumstances, e.g. elements constituting market abuse, any other behaviour or information. Note that it may not always be apparent that a transaction might be abusive

until after a transaction has taken place. However, firms should not breach information barriers to prevent and avoid conflicts of interest in order to detect suspicious transactions/orders.

The FCA has incorporated the STOR requirements of UK MAR into SUP 15.10 of its Supervision Manual and in SUP 15 Ann 5, the FCA has provided some indicators of possible suspicious transactions or orders.

STORs should only be used to report potential market abuse under Article 16 of UK MAR, not other types of suspicion or incidents.

Currently, the Firm and its ARs do not arrange or execute any relevant transactions. If an AR were to do this and a suspicious transaction/order was encountered, a STOR should be made by email to the Firm's MLRO or Deputy MLRO who will make the report to the FCA on behalf of the AR. When initially making the internal STOR, please include the following details and attach relevant supporting documentation:

- Transaction/order number.
- Description of the nature of the suspicion.
- Identity/identifying details of entity/person suspected.
- Additional information.

For more information on suspicious transaction and order reporting, market abuse risks, transaction reporting, and other market conduct issues, refer to the FCA's Market Watch newsletters.

The UK applies an 'all crimes' approach to money laundering meaning that insider dealing and market manipulation are predicate offences to money laundering. Therefore, the Firm, ARs and associated individuals need to also consider their obligations under POCA and TA including the submission of a SAR as well as a STOR to the MLRO and tipping off.

4.3.9 Manager's Transactions

UK MAR Article 19 requires persons discharging managerial responsibilities within certain issuers (PDMRs), and persons closely associated with them (PCAs), to notify the FCA and the issuer of relevant personal transactions they undertake in the issuer's shares, debt instruments, derivatives, or other linked financial instruments, if the total amount of transactions per calendar year has reached €5,000. The issuer in turn must make that information public within 2 working days of receipt of the notification from the PDMR.

This requirement applies to:

- Issuers who have requested or approved admission of their financial instruments to trading on a UK regulated market.
- In the case of instruments only traded on a UK MTF or on a UK OTF, issuers who have approved trading of their financial instruments on a UK MTF or a UK OTF or have requested admission to trading of their financial instruments on a UK MTF.
- UK EAMPs (emission allowance market participants) in relation to transactions in UK emission allowances and related auction products and derivatives.

Given the business model of the Firm and its ARs and the instruments in which they deal, it is considered that notifications under Article 19 of UK MAR do not apply to the Firm or its ARs.

4.3.10 Significant Short Positions

The EU Short Selling Regulation (EU SSR) and Level 2 Regulation were converted into UK law along with Binding Technical Standards at the end of the transition period forming the UK's Short Selling Regulation (UK SSR).

The UK SSR applies to the short selling of sovereign debt, shares that are admitted to trading on a UK trading venue, and related instruments, and the use of credit default swaps (although an exemption for shares exists where the principal trading venue of a share is located in a third country).

It requires holders of net short positions in shares admitted to trading on a trading venue in the UK (unless they are exempt) or UK sovereign debt to make notifications to the FCA once certain thresholds have been breached. Further information on notification and disclosure of net short positions is available from the FCA. The UK SSR also outlines more restrictions on investors entering into uncovered short positions in shares or UK sovereign debt.

The UK SSR provides for certain exemptions for market-making activities and primary market operations. However, the FCA points out that the exemptions cannot be automatically used, are limited and only apply to specific instruments. For further information, see the FCA's note on the UK notification process for market makers and authorised primary dealers under the UK SSR.

The FINMAR section of the FCA Handbook applies to all natural and legal persons to whom the short selling regulation applies.

Under FINMAR 2.5, the FCA may take measures to prohibit, restrict, manage or limit transactions in short positions. This will depend upon a number of different factors as detailed in FINMAR 2.5. Where this is imposed the Firm and its ARs will comply with any current requirements where relevant. However, given the business models of the Firm and its ARs, the SSR is unlikely to apply and where it does the Firm is unlikely to have any significant short positions in the majority of situations.

4.3.11 Risk Assessment

Given the nature of the Firm's business, the Firm views its market conduct risk to be low. However, the Firm recognises that staff may receive inside information in the following situations:

- During the fund close process when the Firm is acting as AIFM or sub-manager and reviewing information provided by prospective investors.
- When reviewing investment advice/recommendations as part of monitoring/oversight but also when acting as AIFM/sub-manager.
- When answering ad hoc queries from ARs or enquiries from prospects/other clients.
- When reviewing independent/non-independent research papers prior to issue.

The Firm considers that, in addition to the above scenarios, ARs may also receive inside information when:

- Researching investments.
- Providing investment advice to, or arranging investments for, listed or soon to be listed companies, either directly or indirectly.
- Conducting due diligence on potential portfolio targets or new mandates/clients/investors.
- A portfolio company becomes listed or becomes the target of a listed entity.

ARs should consider their market conduct risks as part of their firm-wide risk assessments and should put in place processes that complement (but not replace) the Firm's policy and procedures below. This risk assessment should be reviewed quarterly.

4.3.12 Policy and Procedure

The FCA expects senior management to take responsibility for its firm's measures in relation to insider dealing and market manipulation. This includes:

- Understanding the risks of insider dealing/market manipulation that their firm is exposed to (through staff member and client activity).

- Establishing adequate policies and procedures to counter these risks in accordance with SYSC 6.1.1R.

Each staff member and Approved Person shall be given access to a copy of this Manual, which contains a summary of the UK's Insider Dealing Regulations and Market Conduct Rules in the FCA's Handbook upon joining the Firm. It is the responsibility of ARs, and the nominated senior managers specifically, to decide who within their firms should be provided with access to the Manual, required to sign the compliance undertaking, and undergo relevant training as part of induction and annually thereafter.

No individual (director, partner, employee or member of staff) should agree to become an insider in relation to the securities of any company other than where this is *necessary* to perform their role as an investment professional of the Firm. **If an individual feels it necessary to become an insider in order to properly perform their professional role, *advance* notification of this intention should be made using the procedure outlined below. The Firm's Compliance Officer will enable the individual to be compliantly 'wall crossed' (see below) and the security to be added to the insider or restricted lists**. All instructions from the Compliance Officer must be followed completely, correctly, and promptly. The individual should also follow any wall-crossing obligations of the company/party involved.

No member of staff should behave in a way that amounts to market abuse. If in doubt, then guidance should be sought from the Compliance Officer.

Staff members should be aware that they may be made an insider in meetings/conversations and if it is the case that they do not wish to be restricted from dealing in the relevant shares, they should make the other party aware that they do not want to be given inside information.

Staff members should also be aware that information provided to an individual may become inside information by virtue of other information they already hold.

In the event that they do come into possession of inside information and pre-clearance was not possible, they must report this as per the procedure below. The Compliance Officer will add the security to the insider or restricted lists. They must also follow the directions of other compliance/legal departments connected to the transaction for which they have been made an insider.

No individual may personally deal in any security about which the Firm has inside information and is listed on the insider list or restricted list. In advance of any personal dealing, individuals should check the restricted list and follow instructions in Appendix F1.

No individual may reveal any inside information held by the Firm/an AR to any third party unless it is proper and necessary to do so, and they have advance consent from the Firm's Compliance Officer.

The CJA's provisions and FCA Market Conduct Rules are very complex and, if anyone is in any doubt whether a particular transaction would be prohibited, they should consult the Compliance Officer.

It should be noted that any contravention of the insider dealing legislation may result in summary dismissal without notice or compensation and immediate withdrawal of FCA Approved Person status, where applicable. The FCA and the Firm may discipline staff members that are in breach of UK MAR and the FCA's Market Conduct Rules.

4.3.13 Insider List Procedure

Wall-crossing is the practice of bringing individuals over an information barrier, or 'wall', to confidentially share non-public information about a public security offering before the information is announced to the public.

If/when AR staff come to possess any inside information, ARs must inform either their Primary Contact, who will inform the Compliance Officer, or the Compliance Officer, in advance where possible. Firm staff must inform the Firm's Compliance Officer, without delay, including where advance consent has been sought by the external party.

Upon notification from an AR, the Compliance Officer or Primary Contact under the direction of the Compliance Officer, will send a wall-crossing notice to the wall-crossed individuals at the AR and update the restricted list. The Firm's Compliance Officer will update the Firm's own insider list. Once the inside information has become public (or 'stale'), the AR should notify the Compliance Officer or Primary Contact who will confirm this, update the Firm's restricted list, and then send a 'cleansing notice' to the wall-crossed individuals to confirm they are no longer insiders in respect of a particular security and instruct them to update their own insider list. The Firm's Compliance Officer will, as before, update the Firm's insider list.

Information on who is an insider within the Firm and within ARs (insider list) **must** be kept confidential.

The Compliance Officer is responsible for maintaining the insider list and ensuring that Firm staff have access to inside information on a need-to-know basis. Therefore, completion of the confidential insider list can only be delegated to the Deputy Compliance Officer in the Compliance Officer's absence. Whereas restricted lists and other associated admin may be delegated by the Compliance Officer to a compliance team member, such as the Primary Contact.

The Compliance Officer is also responsible for monitoring Firm staff's personal account dealing.

The nominated senior managers at each AR are responsible for monitoring personal account dealing within their ARs and raising any questions or concerns with their Primary Contact or the Firm's Compliance Officer.

The Compliance Officer, other partners, Compliance Manager and compliance associates are super-insiders, i.e. always insiders due to their involvement in each transaction. However, where applicable, i.e. where inside information is received outside of, or separately to, an individual's role for the Firm, the Firm's staff will notify the Firm's Compliance Officer, and the wall-crossing and subsequent cleansing notices, and the updating of both the restricted and insider lists, at the appropriate time, will be issued/updated by the Firm's Compliance Officer.

4.4 Fraud

Fraud is the act of obtaining by deception money or assets belonging to another which will benefit the fraudster and expose the victim to a loss. Fraud may be committed against individuals and firms, e.g. through:

- The use of false or stolen identities to defraud financial services organisations.
- The use of the internet, e.g. setting up websites purporting to belong to a reputable institution.
- The use of phishing emails, texts or phones calls purporting to be from a known connection or offering something.

The FCA requires firms to take reasonable care to establish and maintain effective systems and controls for countering the risk that they might be used to further financial crime.

For the following reasons, the Firm assesses its fraud risk to be low-moderate:

- Its core business is a non-retail regulatory incubation model and the provision of investment management services.

- Its direct client base is comprised of corporate entities that are led by FCA-approved industry professionals.
- Most communications and activities take place online/using the internet, through emails, Teams and Zoom, which increased during the pandemic and has remained at a higher level than before the pandemic.
- The Firm's Managing Partner will, where circumstances permit, meet potential clients face-to-face before proposing them as a new client and before onboarding. In all other cases, meetings will be conducted remotely via video call.
- The Firm thoroughly vets its ARs and ARs' senior management prior to them being appointed.
- Fund ARs are typically required to appoint a recognised and appropriately authorised administrator and manager for each fund.
- Fund ARs are required to instruct a specialist fund lawyer to assist them with all legal aspects of the fund.
- The Firm does not hold or control client money or other assets.
- The Firm does not operate any sales-driven/volume-based incentive schemes.
- When acting as fund manager, the Firm requires:
    - Investors to sign a Professional Client notice confirming they qualify as a Professional Client and are happy to be categorised as such.
    - Investors to be subject to appropriate KYC/AML checks by fund administrators and for the Firm to have final approval for each proposed investor before acceptance into the fund.
    - Fund advisers to conduct extensive due diligence on proposed investments including on the target company's policies and AML/KYC checks on founders.
    - Investment recommendations to include detailed information about the proposed investment including identifying information about the target company and the industry/market in which the target company operates and its founders/key personnel.
    - Fund advisers to properly monitor use of funds by portfolio companies.
- Funds managed by the Firm normally include one or more large, institutional investors in the first close.
- Higher risk relationships at AR and Principal levels need to be approved in advance by the Firm's senior management.

4.4.1 Fraud Indicators

The following situations may require enhanced due diligence and or/reporting:

- Remote (non-face-to-face) clients.
- Failure/unwillingness to provide name and address ID.
- Lack of photographic name ID.
- Third-party client referrals.
- Unusual/unreasonable client behaviour/transactions.
- Investments advertising exceptionally high returns.
- Investments with celebrity endorsements.
- Investments concerning luxury items.
- Investments in high-risk jurisdictions.
- High net worth private clients.
- Unsubstantiated claims of company performance.
- Use of, or requests to change account details to, accounts with ambiguous names or unconnected third parties for receipt of funds or distributions.
- Requests from investors to transfer interests shortly after closing.

- Unexpected communications instructing action or requesting assistance or offering a benefit. These communications can be from unknown sources or known contacts or purporting to be from known sources, e.g. hacked accounts.

4.4.2 Preventing Fraud

There are numerous ways the Firm protects itself against fraud, which include:

- Established and clear reporting lines.
- Regular analysis and discussion of risks.
- Appropriate and documented internal procedures covering all areas of the business.
- Identifying the source of payments from bank details, electronically (using Xero) and manually.
- Thoroughly investigating requests from investors to change/update information or transfer rights.
- Segregation of duties.
- Thorough and risk-based initial and periodic screening of staff members and agents/ representatives and checks, where relevant, to ensure ARs and individuals meet the FCA's fit and proper test criteria initially and on an ongoing basis.
- Sign-off of new clients, and their associated individuals, at partner level prior to FCA submission.
- Sign-off of high-risk relationships at senior manager level.
- Anti-bribery and corruption guidance.
- Staff training and testing, including on phishing communications and other scams.
- Compliance monitoring programme.
- Detailed and risk-based KYC procedures.
- Robust IT security measures.
- Data protection procedures.
- Circulation of FCA enforcement cases, including those relating to fraud, internally and to its ARs in the form of its monthly newsletter.

More information on counter-fraud measures/activities is available from the following organisations:

- The National Fraud Authority.
- The National Fraud Authority's cross-sector strategy, Fighting Fraud Together, which is endorsed by the FCA.
- Action Fraud, the UK's national fraud and cybercrime reporting centre.
- The City of London Police, which has 'lead authority' status in the UK for the investigation of economic crime, including fraud.
- The Fraud Advisory Panel, which acts as an independent voice and supporter of the counter-fraud community.

If staff members are targeted by fraudsters at work, they should report the incident to the Compliance Officer or MLRO who will report the issue to Action Fraud or the Police. A report may also need to be made report to the Firm's insurer.

If an AR is targeted by fraudsters, , it should report this to the Compliance Officer or MLRO. The AR should then make a report to Action Fraud or the Police. As above, the AR may need to inform their insurer. The AR should keep the Compliance Officer or MLRO updated on developments.

4.5 Data Security

4.5.1 Background

The Data Protection Act 2018 sets out the framework for data protection law in the UK and the UK General Data Protection Regulation (UK GDPR) sets out the key principles, rights and obligations for most processing of personal data in the UK, except for law enforcement and intelligence agencies.

The UK GDPR and Data Protection Act 2018 (Part 2, General Processing Regime) require the Firm/ARs to implement and maintain adequate policies and procedures regarding data security. The ICO provides guidance on data protection requirements and the responsibilities imposed on data controllers and data processors.

Chapter 5 of the FCA's Financial Crime Guide contains practical assistance and information for firms of all sizes and across all FCA supervised sectors on actions they can take to counter the risk that they might be used to further financial crime in relation to data security.

4.5.2 Risks

Customers and employees regularly provide firms with important personal/sensitive data. If this data is obtained by criminals, they can attempt to use it to their advantage (and the customer's detriment) such as by undertaking transactions in a customer's/employee's name. The Firm and its ARs should be alert to the financial crime risks associated with holding personal or sensitive data and must take special care of it.

4.5.3 Key Principles and Policy

Every business is different and the Firm and its ARs should, therefore, ensure that they have their own specific data security policy appropriately tailored to their business activities and the data they hold. The policy should cover the core principles of the Data Protection Act which are:

1. Lawfulness, fairness and transparency.
2. Purpose limitation.
3. Data minimisation.
4. Accuracy.
5. Storage limitation.
6. Integrity and confidentiality.
7. Accountability.

In addition, please see below for some self-assessment questions that the Firm/ARs should consider when reviewing its policies and procedures:

- How is responsibility for data security apportioned?
- Has the business ever lost personal/sensitive data? If so, what remedial actions did it take? Did it contact customers? Did it review its systems?
- How does the business monitor that suppliers of outsourced services treat personal/sensitive data appropriately?
- Are data security standards set in outsourcing agreements, with suppliers' performance subject to monitoring?

4.5.4 Systems and Controls

The Firm and its ARs should ensure they put in place systems and controls to minimise the risk that their operation and information assets might be exploited by thieves and fraudsters. Internal procedures such as

IT controls and physical security measures should be designed to protect against unauthorised access to personal/sensitive data. The ICO has published a practical guide to IT security for small firms, but in simple terms security measures should ensure:

- Only authorised people can access personal data.
- Those people can only act within the scope of their authority.
- Where data loss occurs targeted action can be taken quickly to prevent/minimise damage and distress to the individuals concerned.

The ICO has also published a set of 10 quick steps to help businesses improve basic personal/sensitive data security:

1. Take care when printing and copying.
2. Double-check letters/emails before sending.
3. Include a return address on envelopes.
4. Disable auto-fill in your email settings.
5. Close your messaging when screen-sharing or presenting online.
6. Lock your screen when you are away from your desk.
7. Do not let staff share passwords.
8. Send electronic documents securely (e.g. using encryption or password-protection).
9. Send passwords to protected documents separately.
10. Keep your IT systems up to date.

4.5.5 Best Practices

Below are some best practices that the Firm/ARs should ensure their staff are aware of:

- Lock screen.
- Clear desk/office.
- Over-looking.
- Passwords – most secure formats and frequency of change.
- Personal devices – might be within scope of subject access request.
- Data outputs and transfers.
- Removable media – encryption and other conditions of use.
- Remote working – storage and destruction of paper files or documents/notes and electronic devices, do not leave unattended or in plain sight either in a vehicle or in a remote-working location (including at home, in a hotel room or on public transport).

4.5.6 Data Controllers & Data Processors

All ARs are considered by the Firm to be joint data controllers or data controllers in common. If a breach is discovered, the AR/Firm must notify the other and the ICO (where appropriate) within 72 hours. Data processors are required to notify data controllers of all breaches without undue delay.

4.5.7 Penalties

The maximum penalty for a data breach is up to 4% of annual turnover or €20m (whichever is larger).

4.6 Anti-Money Laundering, Counter-Terrorist Financing and Counter Proliferation Financing

4.6.1 Introduction

Money laundering is the process by which criminals attempt to conceal the true origin and ownership of the proceeds of their criminal activities. When successful, money laundering enables criminals to maintain control over their proceeds, and ultimately may provide a legitimate cover for their source of income.

The offence of terrorist financing is made up of 2 parts: money generated by acts of terrorism and money intended for use in acts of terrorism.

Proliferation financing is defined by the FATF as the provision of funds or financial services used for the manufacture, acquisition, possession, development, export, trans-shipment, brokering, transport, transfer, stockpiling or use of chemical, biological, radiological or nuclear (CBRN) weapons and their means of delivery and related materials (including both technologies and dual-use goods used for non-legitimate purposes), in contravention of national laws or, where applicable, international obligations.

The importance of efforts to tackle these activities is related to the FCA's operational objectives as referred to in Chapter 1 including 'Protecting and enhancing the integrity of the UK financial system'.

The current primary legislations in the UK concerned with anti-money laundering, counter-terrorist financing and counter-proliferation financing (AML/CTF/CPF) are POCA (as amended including by Serious Organised Crime and Police Act 2005), TA (as amended), which outline the money laundering and terrorist financing offences, and the Sanctions and Anti-Money Laundering Act (SAMLA). In addition, the MLRs 2017 impose obligations on those performing regulated activities.

4.6.1.1 POCA

Under POCA there are 5 basic criminal offences with the penalty for non-compliance ranging from 5 years to 14 years' imprisonment, a fine, or both.

1. **Concealing or transferring criminal proceeds**. Attempts to convert or disguise the proceeds of crime into something appearing legitimate, or transferring money to avoid detection or confiscation, are criminal offences.
2. **Assisting others to launder money**. It is a criminal offence to help others to launder money. 'Assisting' can be any kind of assistance, active or passive.
3. **Acquiring, possessing or using criminal proceeds**. If it is known that money is directly or indirectly the proceeds of a crime, it is an offence to receive, possess or use that money. 'Money' has a wide definition, including property.
4. **Failing to report actual or suspicious money laundering activity**. The duty is on the individual to prove that there were no grounds for suspicion. It is also a criminal offence not to report promptly where there are reasonable grounds for suspicion.
5. '**Tipping off**'. It is a criminal offence to alert a suspected money launderer or accomplice of the fact that an investigation is underway, or report has been made into suspected money laundering.

It is important to note that the POCA offences involve the proceeds of any criminal behaviour, by anyone, anytime, anywhere. This means that funds generated by activities in breach of FSMA would be in scope of POCA. There is, however, one exception to the 'all crimes' application, which is where it is known or there are reasonable grounds to believe that the conduct occurred outside the UK in a jurisdiction in which it was legal under recognised local law.

4.6.1.2 Terrorism Act

Part III of the TA contains offences, including money laundering offences (s18), and imposes an obligation on firms to make reports where they know or suspect, or have reasonable grounds to suspect, engagement in terrorist financing:

- Offences for fund-raising (s15), using and possessing (s16), and arrangements concerned with funding terrorism or controlling terrorist property (s17).
- Specific offence for insurers regarding insurance payments made in response to terrorist demands (s17A).
- Failing to disclose knowledge or suspicion of terrorist financing (s21A).

4.6.1.3 Sanctions and Anti-Money Laundering Act

The SAMLA enabled the UK to create its own sanctions framework and money laundering and terrorist financing regulations autonomously post-Brexit. Numerous sanctions regimes aimed at countering proliferation financing are implemented by this Act.

4.6.1.4 The Money Laundering, Terrorist Financing and Transfer of Funds (Information on the Payer) Regulations 2017 (MLRs 2017)

The MLRs 2017 contain 3 separate criminal offences:

- Contravening a relevant requirement (regulation 86).
- Prejudicing an investigation (regulation 87).
- Providing false or misleading information (regulation 88).

The MLRs 2017 also place a legal requirement on firms to follow a **risk-based approach**, both in respect of risk management generally, and specifically in respect of KYC/AML due diligence measures. The Firm and its ARs are required to take appropriate steps to identify and assess money laundering, terrorist financing and proliferation financing risks, to document risk assessments and keep them up to date. A third party such as an auditor or regulator should be able to understand the decisions made by the Firm/AR from its records.

In assessing financial crime risk, the MLRs 2017 require the Firm to take account of:

- The risks from:
    - Customers and underlying beneficial owners.
    - Products/services.
    - Transactions.
    - Delivery channels.
    - Geographical areas of operation.
- Information made available to them by the FCA, including enforcement findings and consequential actions.
- Risk factors, including factors relating to its customers, countries or geographic areas in which they operate, products, services, transactions and delivery channels.
- Relevant findings in the UK National Risk Assessment of Money Laundering and Terrorist Financing policy paper.
- The UK's National Risk Assessment of Proliferation Financing.
- Advisory notices issued by UK authorities.

The Firm should also be aware of the Home Office's Serious and Organised Crime Strategy last updated in November 2014.

The MLRs can be enforced by both criminal and civil penalties.

4.6.2 FCA Expectations

The FCA expects firms, including ARs, to follow the rules contained in the SYSC sourcebook, which are intended to drive an effective, risk-based approach. The SYSC provisions place emphasis on the detailed guidance contained within the Joint Money Laundering Steering Group's (JMLSG's) Guidance which supports firms in meeting their obligations to follow a risk-based approach under the UK AML/CTF regime. The FCA will take into account whether a firm has followed the provisions contained in the guidance. The Firm also recognises the FCA's Financial Crime Guide, which, along with the JMLSG guidance, is considered 'relevant guidance' as described in Regulations 76(6) and 86(2) of the MLRs 2017. Guidance is updated from time to time, so it is advisable to view guidance at source to ensure the latest version is being used.

The FCA's webpage on the MLRs covers the main aspects of the UK's anti-money laundering regime from a regulatory perspective.

The Firm must put in place and operate arrangements that enable it to comply with AML/CTF/CPF legislation. Kevin Gallacher is the senior manager responsible for operational systems and controls to prevent financial crime. Emma Jones is the MLRO. The MLRO is responsible for the oversight of the Firm's AML activities, and is the key person in the implementation of the Firm's AML/CTF/CPF strategies and policies. Gillian Gallacher, Partner and Compliance Officer, is the Firm's Deputy MLRO. **ARs' policies and procedures should incorporate/reflect the controls and roles at principal level.**

Money laundering risk is defined as the risk that a firm may be used to facilitate money laundering. Failure by a firm to manage this effectively will increase the risk to society of crime and terrorism. The MLRO is responsible for ensuring financial systems and controls are in place to take adequate notice of the risk of money laundering to which the business is exposed, and shall report to the partners regularly.

The Firm and its ARs are also required to mitigate the risk of terrorist and proliferation financing.

There is a high degree of commonality between the AML, CTF and CPF regimes. Indeed, the FATF's 40 recommendations cover all but 3 are specific to CTF (Recommendations 5, 6 and 8) and Recommendations 1, 2, 7 and 15 which have been expanded to also cover PF. As such, the AML measures firms put in place can also be used mitigate the risk of TF and PF. However, there are key differences between all 3, for example:

1. Often only small amounts needed to commit terrorist acts and moderate amounts used for proliferation activity, but large amounts often involved in money laundering.
2. Terrorism can be funded from legitimately obtained income.
3. Proliferation often involves state-sponsored programs.
4. Detection focus for proliferation is on individuals, entities, states, goods and materials and transactions often look like normal commercial activity, but structured to hide origin of funding. Whereas, money laundering typically involves a complex web of transactions often involving shell companies and offshore secrecy havens.
5. The money trails for TF and PT tend to be linear but ML money trails are often circular eventually ending up with the person who generated the funds.

Sources of information on TF and PF risks include: press reports; OFSI alerts; NCA alerts; FATF typologies; and court judgements.

4.6.3 AML Systems & Controls

SYSC 6.3.1 R requires the Firm to have in place systems and controls that:

1. Enable it to identify, assess, monitor and manage money laundering risk.
2. Are comprehensive and proportionate to the nature, scale and complexity of its activities.

SYSC 6.3.3 R requires the Firm to carry out regular assessments of the adequacy of its systems and controls.

In identifying its money laundering risk and in establishing the nature of its systems and controls, a firm should consider a range of factors, including:

1. Its clients, products and activity profiles.
2. Its distribution channels.
3. The complexity and volume of its transactions.
4. Its processes and systems.
5. Its operating environment.

The partners have assessed the Firm as being at low risk from a money laundering perspective for the following reasons:

- The Firm's business consists of providing investment management services to Professional Clients (funds) and not Retail Clients.
- The associated money laundering risks relate to the transfer and redemption of money/funds to and from the funds and from its ARs (monthly fee).
- The Firm's deals with low volumes of high value clients/funds and has an in-depth relationship with each client.
- The client take-on process involves a detailed understanding of the client's needs and priorities and anticipated inflows and outflows of funds in order to determine suitable investment parameters. The Firm usually maintains ongoing contact with its clients in order to review market developments and performance.
- Given the nature of the Firm's business, it expects to be remunerated by its clients for its services via bank transfers or cheques. It would be very unusual to receive cash payments or payments from unrelated third parties; and any such requests for payments will be subject to further enquiries.
- The Firm's client base is generally located in comparable jurisdictions with adequate AML standards.
- Any changes in the business are reviewed on a regular basis by the Compliance Officer and the risks are reconsidered.

ARs should carry out and document their own risk assessments.

Regulated firms are also required to undertake risk assessments prior to the launch of new products or business practices including in new jurisdictions, as well as new technologies. Firms should review risk assessments in response to material changes and developments.

4.6.4 Reporting Suspicions of Money Laundering

4.6.4.1 Main Obligations

Staff of the Firm and ARs must report any suspicious activities to the MLRO, whose responsibility it is then to determine whether or not a report should be made to the NCA. In the absence of the MLRO, this should be made to the Deputy MLRO. The Firm's staff may be disciplined if they fail without reasonable excuse to report potentially suspicious activity. Senior management of the Firm/ARs must permit the MLRO to:

1. Have access to any information in the Firm's/AR's possession that could be relevant.
2. Make a report without the approval of any other person.

4.6.4.2 The SAR Regime

- If a step that needs to be taken in a relevant transaction or matter would fall within sections 327 to 329 of POCA, the member of staff will need appropriate consent from the NCA before taking that step. 'Appropriate consent' is defined in section 335 of POCA. The MLRO should seek consent from the NCA at the same time as submitting the SAR.

- If NCA consent is needed, the member of staff must not take any further substantive action unless or until the consent is received and communicated to the member of staff by the MLRO. However, this will not prevent the staff member from progressing the matter otherwise (e.g. in writing letters or conducting searches), **provided they do not commit the tipping-off offence**.
- The initial notice period is **7 working days** from the day after receipt of the consent request. If the NCA refuses consent, the entity is subject to a moratorium period of 31 days, at which point deemed consent applies.
- The NCA can apply for 31-day extensions to the moratorium period of up to 186 days in total past the original 31-day period expiry date.
- The Criminal Finances Act (CFA) allows greater information sharing within the regulated sector, subject to the conditions set out below (from s339ZB of the POCA 2002) being satisfied, permitting one firm in the regulated sector to disclose information to another, whether or not requested to do so by the other firm, or on request or with the permission of the NCA. **Only the MLRO or Deputy MLRO can request disclosure and any disclosure requests must be sent to the MLRO/Deputy MLRO without delay**.
    - Condition 1 is where —
        a. A is carrying on a business in the regulated sector as a relevant undertaking.
        b. The information on which the disclosure is based came to A in the course of carrying on that business.
        c. The person to whom the information is to be disclosed (or each of them, where the disclosure is to more than one person) is also carrying on a business in the regulated sector as a relevant undertaking (whether or not of the same kind as A).
    - Condition 2 is that —
        a. An NCA authorised officer has requested A to make the disclosure or,
        b. The person to whom the information is to be disclosed (or at least one of them, where the disclosure is to more than one person) has requested A to do so.
    - Condition 3 is that, before A makes the disclosure, the required notification has been made to an NCA authorised officer (see section 339ZC(3) to (5)).
    - Condition 4 is that A is satisfied that the disclosure of the information will or may assist in determining any matter in connection with a suspicion that a person is engaged in money laundering.
    - A person may disclose information to A for the purposes of making a disclosure request if, and to the extent that, the person has reason to believe that A has in their possession information that will or may assist in determining any matter in connection with a suspicion that a person is engaged in money laundering.
    - The Act also sets out in s339ZC other conditions such as, the information the disclosure request must contain including that it must identify the person suspected of money laundering (if known) and the information it seeks, as well as details of the person who should receive the information. Where relevant, the request must also include the information the recipient firm would need in order to assess whether or not disclosing the information would meet the test of assisting in connection with a suspicion.
- The CFA enables the submission of joint/super SARs. However, whether or not to submit a joint/super SAR is the decision of the MLRO/Deputy MLRO. Staff members of the Firm and ARs should submit a SAR, as required, to the MLRO/Deputy MLRO in the first instance. For further information, please refer to the Home Office Circular issued in February 2018 on the sharing of information within the regulated sector, and between the regulated sector, the police and the NCA.
- The NCA can request further information from the person who made the disclosure, or any other persons in the regulated sector, following receipt of a SAR.

4.6.5 Government and International Findings

The Firm is required to obtain and act on findings issued by the UK government or an internationally accredited organisation of which the UK is a member, such as the FATF.

These findings will be published when the government, a government department or the FATF has examined money laundering prevention arrangements in a jurisdiction other than the UK and has found those arrangements to be materially deficient from relevant international and accepted standards. The FATF's latest (2018) Mutual Evaluation Report on the UK can be accessed here.

4.6.6 Risk-Based Approach

The Firm's risk-based approach categorises clients as either low, medium or high risk and requires the application of KYC measures and monitoring appropriate to the overall level of risk posed by the individual/entity. Whatever the approach taken, the broad objective is that prior to establishing a business relationship, the Firm/AR must know at the outset of the relationship:

- Who its customers and, where relevant, the controllers and/or beneficial owners of its customers, are.
- Where they operate.
- What they do.
- The source of their funds (the origin of the funds involved in the business relationship or occasional transaction).
- The source of their wealth (how they acquired their total wealth).
- Their expected level and type of activity.

The above analysis must be documented.

The Firm/AR must apply appropriate, risk-sensitive customer due diligence (CDD) measures on customers when it does any of the following:

- Establishes a business relationship.
- Carries out an occasional transaction.
- Suspects money laundering or terrorist financing.
- Doubts the veracity of documents, data or information previously obtained for the purpose of identification or verification.

Where the client is a legal person, trust, company, foundation or similar legal arrangement, there is a specific requirement under the amended MLRs to take reasonable measures to understand the ownership and control structure of that client. Whilst beneficial ownership is clearly defined in the MLRs 2017, control is not. However, reference to Persons with Significant Control (PSC) information on Companies House is referred to. Therefore, PSC information and regulatory definitions of controllers should also be considered on a case-by-case basis.

The General Rule (Regulation 30(2) for the MLRs 2017) states that the verification of the identity of the client and, where applicable, the beneficial owners (and controllers), must, unless an exception applies, take place before the establishment of a business relationship or the carrying out of an occasional transaction.

The level of due diligence that is appropriate will depend on the level of risk posed by the prospective client taking into account numerous factors. The Firm should assess the risk posed by each client on a case-by-case basis, assigning appropriate weighting to relevant risk factors in order to produce an overall risk rating/profile for each client, having full regard to the high-risk factors contained in Regulation 33 of the MLRs 2017 (as amended in 2019). When weighting factors, the Firm should ensure:

- Weighting is not unduly influenced by just one factor.
- Commercial considerations do not inappropriately influence the risk assessment.
- Situations identified by national legislation or risk assessments as always presenting a high money laundering risk cannot be overruled by the Firm's weighting.
- The Firm is able to override any automatically generated risk scores where necessary. The rationale for the decision to override such scores should be documented appropriately.

Annex 4-II of the JMLSG Guidance Part 1 contains a fuller list of illustrative risk factors a firm may address when considering the money laundering/terrorist financing risk posed by customer situations, which is consistent with the Risk Factor Guidelines issued by the ESAs.

Section 5 of Part 1 of the JMLSG Guidance sets out how to properly verify the identity of different types of person. The UK government's webpage How to prove and verify someone's identity also contains some useful guidance.

Written records of all due diligence actions taken should be kept, especially where there have been difficulties in identifying beneficial owners, for at least 5 years from the end of the business relationship or from the date of the occasional transaction. See Regulation 28 (7) and (8) of the MLRs for more information on beneficial ownership requirements and difficulties.

Examples of clients/characteristics that are likely to fall within low, medium or high risk are listed in the following sections but each client should be judged on a case-by-case basis.

4.6.6.1 Low Risk

- Regulated financial institutions based in the UK; those located in EU, FATF or comparable jurisdictions.
- Government offices and agencies in all jurisdictions except for those in the non-cooperative countries and territories (NCCTs).
- Companies or their subsidiaries (50% or more) whose shares are traded on a UK or EU regulated market or equivalent exchange.
- Reputable, well-known organisations, with long histories in their industries or large market capitalisation and with substantial public information about them and their principals and/or controllers.
- Clients represented by those whose appointment is subject to court approval or ratifications (e.g. executors).

4.6.6.2 Medium Risk

All other clients that do not fall within either a low-risk category or a high-risk category including (but not restricted to):

- Subsidiaries of or entities associated with low-risk clients.
- Private companies from the UK, EEA or comparable jurisdiction provided they are not undertaking high-risk business.

In the absence of high-risk indicators the Firm's clients are expected to be private companies and individuals who will be categorised as medium risk.

For private companies the Firm/AR may obtain the following information from an independent source such as Companies House or from a reputable business information provider:

- An official document containing the client's full name and registered number.
- Evidence of client's registered office in the country of its incorporation.
- Evidence of client's business address.
- Its articles of association or other governing documents.

- Names of all directors or members of the management body.
- Names of all direct and indirect beneficial owners owning 25% or more of the entity.
- Names of any individuals who otherwise exercise control over the management of the company.
- Copy of latest audited accounts where available.
- Evidence of group ownership (e.g. sufficiently detailed structure chart), where relevant.
- The identity of at least one director must be verified via a certified passport or driving licence copy and a recent (dated within the last 3 months) utility bill or active bank account statement.

For clients that are individuals, the Firm/AR must obtain **and verify** their full name, residential address and date of birth and verify using a certified passport or driving licence copy and a recent (dated within the last 3 months) utility bill or active bank account statement.

If the client is a trust or charity, or another legal form, requirements in Part 1 of the JMLSG Guidance should be checked and if queries remain, the MLRO should be consulted to advise on the appropriate client take-on process.

4.6.6.3 High Risk – Requires Advance Approval from Compliance Officer or MLRO

To enable the Firm to consider the risks associated with high-risk clients in the context of its own risk appetite and risk management processes, and to confirm whether or not the risks are acceptable, a client categorised as high risk should be:

- Subject to appropriate, risk-sensitive *enhanced* due diligence measures, including ongoing monitoring where appropriate.
- Subject to adequate measures to establish and verify the source of wealth and source of funds.
- Signed off by the Firm's Compliance Officer or MLRO in advance of services being provided at both the Firm and AR level. Sign-off is provided, where appropriate, on the basis of a review of, and a discussion covering, a file note summarising all relevant risk factors and the complete file to ensure a holistic view is taken of the subject matter. Where the risk profile of a prospective or existing client (or investor or investee), either as part of initial due diligence or as a result of ongoing monitoring, is beyond the Firm's risk appetite, the Compliance Officer and MLRO will issue instructions on how to terminate the relationship. These instructions must be followed.

Examples of high-risk client types, or factors that separately or collectively indicate a client is high risk, are as follows:

- Relationships involving politically exposed persons (PEPs), their family members and/or known close associates:
    - A PEP is defined in the 2017 Regulations as 'An individual who is entrusted with prominent public functions, other than as a middle-ranking or more junior official.'
    - The latest NRA judges wealth management (and private banking) firms to be particularly exposed to the risk of being used to launder the proceeds of political corruption and tax evasion.
    - Prominent public functions include:
        - Heads of state, heads of government, ministers and deputy or assistant ministers.
        - Members of parliaments or of similar legislative bodies.
        - Members of supreme courts, of constitutional courts or of other high-level judicial bodies whose decisions are not generally subject to further appeal, except in exceptional circumstances.
        - Members of courts of auditors or of the boards of central banks.
        - Ambassadors, charges d'affaires and high-ranking officers in the armed forces (other than in respect of relevant positions at Community and international level).

        - Members of the administrative, management or supervisory boards of state-owned enterprises.
        - Directors, deputy directors and members of the board or equivalent function of an international organisation.
    - Public functions exercised at levels lower than national should normally not be considered prominent. However, when their political exposure is comparable to that of similar positions at national level, e.g. a senior official at state level in a federal system, the Firm should consider, on a risk-based approach, whether persons exercising those public functions should be considered as PEPs.
    - Family members of a PEP include:
        - A spouse or partner of that person.
        - Children of that person and their spouses or partners.
        - Parents of that person.
    - Close associates of a PEP include:
        - Any individual who is known to have joint beneficial ownership of a legal entity or legal arrangement, or any other close business relations, with a PEP.
        - Any individual who has sole beneficial ownership of a legal entity or legal arrangement which is known to have been set up for the benefit of a PEP.
    - The Firm is not required to apply enhanced due diligence measures to family members or close associates of a PEP when the PEP is no longer entrusted with a prominent public function, whether or not the one-year period after the PEP has exited the position in question has expired.
    - Also see section 4.8.6.4 below, which covers the FCA's expectations of firms' treatment of PEP relationships.
    - The MLRs 2017 (as amended) require the UK to create and maintain lists of offices and functions that qualify as politically exposed at national level.
- Complex business ownership structures, such as offshore special purpose vehicles, that make it easier to conceal underlying beneficial owners, especially where there is no legitimate commercial rationale.
- Relationships involving clients that reside in or are nationals of NCCTs.
- Business relationships or transactions with high-risk third countries: the MLRs 2017 (as amended by the Money Laundering and Terrorist Financing (Amendment) (High-Risk Countries) Regulations 2021) contain a list of countries considered high-risk in Schedule 3ZA (currently located here). The list will be periodically updated by way of further regulations, e.g. to reflect relevant changes to FATF lists. Therefore, relevant staff members of the Firm/AR must register for updates to keep pace with developments or check the list regularly but particularly as part of onboarding and ongoing monitoring.
- Accounts that involve large and/or regular payments to or from unrelated third parties.
- Where there is evidence of complex or unusually large transactions; or unusual patterns of transactions, which have no apparent economic or legal purpose – in these situations the Firm should as far as reasonably possible examine the background and purpose of the transactions and, should the relationship proceed, apply enhanced monitoring of the business relationship and include a higher degree of scrutiny over transactions.
- Names that have been previously linked with financial crime or other adverse media.
- Clients based in or conducting business in or through high-risk jurisdictions with known levels of corruption and/or organised crime, or drug production and distribution.
- Clients engaged in higher risk business activities.
- Companies issuing bearer shares, especially if incorporated in higher risk jurisdictions.
- Clients that have been subject to a suspicious transaction report.

- Clients that have not been physically present for identification purposes. This does not apply to clients to whom simplified due diligence applies (see below).
- A client that is the beneficiary of a life insurance policy.
- A client that is a third-country national seeking residence rights or citizenship in exchange for transfers of capital, purchase of a property, governments bonds or investment in corporate entities.
- Transactions without certain safeguards, for example, as set out in regulation 28 (19) concerning electronic identification processes.
- Transactions related to oil, arms, military defence, precious metals, tobacco products, cultural artefacts, ivory or other items related to protected species, or archaeological, historical, cultural and religious significance, or of rare scientific value.
- Transactions connected to controlled (see list here) or dual-use items, e.g. carbon fibre, vacuum pumps, electronic components, and testing equipment, which can also be used in the nuclear industry.

4.6.6.4 Politically Exposed Persons – FCA's Expectations of Firms

Individuals who have, or have had, a high political profile, or hold, or have held, public office, can pose a higher money laundering risk to firms as their position may make them vulnerable to corruption. This risk also extends to members of their immediate families and to known close associates.

PEP status itself does not, of course, incriminate individuals or entities. It does, however, put the customer, or the beneficial owner, into a higher risk category.

In respect of PEPs, family members and associates of PEPs, enhance due diligence measures should always be applied and senior management approval will need to be obtained prior to acceptance of the relationship.

The risk presented by PEPs and their connected persons will not always be the same – some factors will mean the associated risk of one PEP is further up the high-risk scale than other PEPs and therefore more extensive checks should be conducted in these situations.

The Firm must take adequate measures to establish the source of wealth and source of funds which are involved in the business relationship in order to allow the Firm to satisfy itself that it does not handle the proceeds from corruption or other criminal activity.

The measures the Firm should take to establish the PEP's source of wealth and the source of funds will depend on the degree of high risk associated with the business relationship, and where the individual sits on the PEP continuum. The Firm should verify the source of wealth and the source of funds on the basis of reliable and independent data, documents or information where the risk associated with the PEP relationship is particularly high.

See training presentation and FCA Guidance for more information on PEPs, including the risk factors to consider and the types of checks to perform.

4.6.6.5 Simplified Due Diligence

Simplified due diligence (SDD) is where, following a risk assessment, it is considered that there is a low risk of money laundering/terrorist financing/proliferation financing (ML/TF/PF) associated with the prospective client.

When assessing whether there is a low degree of risk of ML/TF/PF in a particular situation, and the extent to which it is appropriate to apply SDD measures in that situation, a firm must take account of at least the following risk factors:

- Whether the customer is:

- A public administration, or a publicly owned enterprise.
- An individual resident in a geographical area of low-risk credit or financial institution subject to the requirements in the 4th Money Laundering Directive.
- A company listed on a regulated market.
- An independent legal professional holding pooled accounts.
- Certain life assurance and e-money products (see Part II, sectors 7 and 3).
- Certain pension funds (see paragraphs 5.4.4 and 5.3.208ff).
- Child trust funds and junior ISAs.

Applying SDD might involve:

- Checking with the home country central bank or relevant supervisory body.
- Checking with another office, subsidiary, branch or correspondent bank in the same country.
- Checking with a regulated correspondent bank of the overseas institution.
- Obtaining from the relevant institution evidence of its licence or authorisation to conduct financial and/or banking business.

The Firm, therefore, must have reasonable grounds for believing that the customer falls within one of the categories set out below and maintain a record of this assessment, the initial due diligence and ongoing monitoring (where applicable) for at least 5 years following the termination of the relationship.

SDD may therefore be applied to the following categories of client/investment products:

- Certain other regulated firms in the financial sector.
- Companies listed on a regulated market.
- Beneficial owners of pooled accounts held by notaries or independent legal professionals.
- UK public authorities.
- Community institutions.
- Certain life assurance and e-money products.
- Certain pension funds.
- Certain low-risk products.
- Child trust funds.

SDD measures must not be applied, or continue to be applied, where:

- The Firm's risk assessment changes and it no longer considers that there is a low risk of ML/TF/PF.
- The Firm suspects money laundering or terrorist or proliferation financing.
- There are doubts about the veracity or accuracy of documents or information previously obtained for the purposes of identity or verification.

4.6.6.6 Standard KYC Evidence

Standard KYC evidence can be obtained for firms and individuals that do not meet the criteria for SDD but are not deemed to be higher risk clients, e.g. on a risk-assessed basis, private limited companies and private individuals.

Staff should also refer to the current version of the relevant training material and the template KYC and client categorisation checklist when assessing what information should be obtained from the customer.

Staff should refer to the Firm's KYC Process and Checklist and/or the JMLSG's Part 1 Guidance for a list of acceptable documents for other client types.

4.6.6.7 Enhanced Due Diligence (EDD)

The General Obligation in Regulation 33(1) is that EDD should be applied in any situation that presents a higher risk of money laundering or terrorist financing, or where the information obtained as part of its KYC process is insufficient in relation to the risks presented.

The extent of EDD must be commensurate to the risk associated with the business relationship or occasional transaction but firms can decide, in most cases, which aspects of CDD they should enhance. This will depend on the reason why a relationship or occasional transaction was classified as high risk.

It should be noted that EDD should always be applied to PEPs (including domestic PEPs) and their associated/connected persons. It should also be noted that EDD measures continue to apply to PEPs for a year after they have left office.

In addition to the general obligation referred to above, the MLRs 2017 prescribe 6 specific circumstances in respect of which EDD measures must be applied. These are:

- In any case identified by the Firm under its risk assessment (or in information provided by the supervisory authorities) where there is a high risk of ML/TF/PF.
- In relation to correspondent banking relationships (see JMLSG Guidance Part II, sector 16: Correspondent relationships).
- If a firm has determined that a customer or potential customer is a PEP, or a family member or known close associate of a PEP.
- In any case where a customer has, or is suspected to have, provided false or stolen identification documents or information on establishing a relationship.
- In any case where:
    - A transaction is complex and unusually large.
    - There is an unusual pattern of transactions.
    - Transactions that have no apparent economic or legal purpose.
    - Transactions involving or connected to cryptoassets, controlled or dual-use items.
- In the case of business relationships or transactions involving high-risk third countries, the amended MLRs specifically require firms to apply one or more of the following enhanced CDD measures:
    - Obtaining additional information on the customer and on the customer's beneficial owner;
    - Obtaining additional information on the intended nature of the business relationship;
    - Obtaining information on the source of funds and source of wealth of the customer and of the customer's beneficial owner;
    - Obtaining information on the reasons for the transactions;
    - Obtaining the approval of senior management for establishing or continuing the relationship;
    - Conducting enhanced monitoring of the business relationship by increasing the number and timing of controls applied and selecting patterns of transactions that need further examination.

4.6.6.8 Reliance on Third Parties

Where a firm relies on a third party to carry out CDD measures, it must obtain from the third party all the information needed to identify the customer or beneficial owner.

The Firm must enter into written arrangements with the third-party provider being relied on which:

- Enable the Firm to obtain from the third party immediately on request (or at the latest within 2 working days) copies of any identification and verification data and any other relevant documentation on the identity of the customer or beneficial owner.

- Require the third party to retain copies of the data and documents referred to above for 5 years beginning on the date on which the third party is relied on by the Firm.

There is nothing in the MLRs 2017 that prevents the Firm applying CDD measures by means of an appropriate agent or an outsourced service provider, as set out in the MLRs 2017, provided that the arrangements between the Firm and the agent or outsourced service provider provide for the Firm to remain liable for any failure to apply such measures and the agent or service provider agrees to be relied upon.

Whether a firm wishes to place reliance on a third party will be part of the Firm's risk-based assessment. In practice, the Firm needs to know:

- The identity of the customer or beneficial owner whose identity is being verified.
- The level of CDD that has been carried out.
- Confirmation of the third party's understanding of their obligation to make available, on request, copies of the verification data, documents or other information.

4.6.6.9 Reliance on Electronic CDD Measures

Regulation 28 of the MLRs set out the circumstances under which electronic identification processes may be considered in undertaking CDD measures. Specifically, where these are:

- Independent of the person whose identity is being verified.
- Secure from fraud and misuse.
- Capable of providing an appropriate level of assurance that the person claiming a particular identity is in fact the person with that identity.

See sections 5.3.39-5.3.53 of Part 1 of the JMLSG Guidance for more information on the use of electronic checks.

The Firm's view is that a combined approach of both electronic and manual checks will likely be appropriate in most cases given the Firm's typical client.

4.6.7 Beneficial Ownership

The 2017 Regulations state that a beneficial owner is normally an individual who ultimately owns or controls the customer on whose behalf a transaction is being conducted. In respect of private individuals the customer is the beneficial owner, unless there are features of the transaction, or surrounding circumstances, that indicate otherwise. Therefore, there is no requirement on the Firm to make proactive searches for beneficial owners in such cases, but it should make appropriate enquiries where it appears that the customer is not acting on their own behalf.

The 2017 Regulations define beneficial owners as individuals either owning or controlling more than 25% of body corporates or partnerships or otherwise owning or controlling the customer. These individuals must be identified, and reasonable measures must be taken to verify their identities.

In relation to a trust, the ML Regulations define the beneficial owner as each of:

- The settlor.
- The trustees.
- The beneficiaries, or where the individuals benefiting from the trust have not been determined, the class of persons in whose main interest the trust is set up or operates.
- Any individual who has control over the trust.

In relation to a foundation or other legal arrangement similar to a trust, the beneficial owners are those who hold equivalent or similar positions to those set out in paragraph 5.3.10.

In relation to a legal entity or legal arrangement which does not fall within 5.3.8-5.3.10, the beneficial owners are:

- Any individual who benefits from the property of the entity or arrangement.
- Where the individuals who benefit from the entity or arrangement have yet to be identified, the class of persons in whose main interest the entity or arrangement is set up or operates.
- Any individual who exercises control over the property of the entity or arrangement.

The threshold of beneficial ownership in the MLRs 2017 is 25%. The Firm/AR is required to obtain and hold adequate, accurate and current information on its own beneficial ownership. Authorities and firms should be able to access this information in a timely manner.

Trustees are required to disclose their status when becoming a client and are similarly required to make beneficial owner information available to authorities and firms.

Before establishing a business relationship, the identity of a client or beneficial owner must be verified using corresponding beneficial ownership registers, where available, or otherwise, on the basis of documents or information obtained from a reliable source which is independent of the client. The Firm/AR must take reasonable measures so that it is satisfied that it knows who the beneficial owner is. It is up to the Firm/AR to consider whether it is appropriate, in light of the money laundering or terrorist financing risk associated with the business relationship, to make use of records of beneficial owners in the public domain, ask its client for relevant data, require evidence of the beneficial owner's identity on the basis of documents or information obtained from a reliable source which is independent of the client, or obtain the information in some other way.

As risk dictates, the Firm/AR must undertake reasonable measures to understand the ownership (and control structure) of its customers and retain evidence of the steps taken on file.

Where a firm has not succeeded in identifying the beneficial owner, or is not satisfied that the individual(s) identified is (or are) in fact the beneficial owner(s), as well as that being a finding in itself which the firm should consider as part of its overall risk assessment, the amended Regulation 28 requires the firm to take reasonable measures to verify the identity of senior managing officials of the legal person in question.

Written records of all actions taken to identify beneficial owners and/or senior managing officials, and any difficulties in identifying the same, should be kept for at least 5 years from the end of the business relationship or the date of the occasional transaction.

4.6.7.1 Discrepancies in Registers and beneficial ownership

Subject to certain conditions/restrictions detailed in Regulation 30A of the MLRs, firms are required to report to Companies House (or the equivalent registrar) any discrepancies in PSC (persons with significant control) between the information they collect about a customer as part of initial due diligence before establishing a business relationship, or which becomes available to the firm when complying with the MLRs, and the information held by Companies House (or the equivalent registrar).

Guidance on how to report relevant discrepancies to Companies House can be found here.

From April 2023, the discrepancy reporting obligation is being expanded to the reporting of material discrepancies in beneficial ownership information arising from ongoing CDD obligations including for the Register of Overseas Entities.

4.6.7.2 Trusts

From 1 September 2022, the Regulation 30A of the MLRs will require firms to request proof of the trust's registration with, or an excerpt from, the Trust Registration Service (TRS) register from the client at the outset of the business relationship.

4.6.8 Ongoing Monitoring

Ongoing monitoring means scrutinising activity on a risk-sensitive basis or in certain situations (see below) to ensure that it is consistent with what the Firm/AR knows about its client and taking steps to ensure that the Firm's/AR's knowledge about the business relationship remains current.

Under Regulation 28(11), firms must conduct ongoing monitoring of the business relationship with their clients. The Regulation also states that ongoing monitoring of a business relationship includes:

- Scrutiny of transactions undertaken throughout the course of the relationship (including, where necessary, the source of funds) to ensure that the transactions are consistent with the firm's knowledge of the customer, business and risk profile.
- Ensuring that the documents or information obtained for the purposes of applying CDD are kept up to date.

Part 1 of the JMLSG states that the essentials of a monitoring system, which can be real-time or after the event, manual or automated, are having up-to-date client information on the basis of which it will be possible to spot the unusual, and asking pertinent questions promptly to elicit the reasons for unusual transactions or activities in order to judge whether they may represent something suspicious, and taking appropriate action on the findings.

Monitoring should be appropriate to the frequency, volume and size of transactions with clients in the context of the associated risks.

In accordance with Regulation 33(1), higher risk accounts and client relationships require enhanced ongoing monitoring. This will generally mean more frequent or intensive monitoring. FCG 3.2.9 provides examples of enhanced ongoing monitoring measures.

The Firm uses, and within 24 hours can gain access to, additional software to assist with enhanced ongoing monitoring. All higher risk relationships requiring senior management sign-off are added to the 'watchlist'.

4.6.9 Additional Notes on Client Risk Management

1. The Firm/ARs will not become party to a client relationship except with clients that have been identified in accordance with its own risk-based approach and, where applicable, have been approved by Firm/AR senior management.
2. The Firm/ARs will not do any business with clients of a dubious or criminal provenance.
    - In client relationships, the Firm/ARs will not proceed on the basis of mistrust; however, should the provenance of the client be subject to question or where doubts arise, additional clarifications are necessary before the business can take place.
3. The Firm does not participate in a transaction without an understanding of the economic context.
    - Understanding of the economic context can also include the identification of the financial beneficiary and the placing of the identification on the record if this is required for evaluating the consequences of a transaction.
4. The amended MLRs require the Firm/AR to examine the purpose and background of all transactions that fulfil at least one of the following conditions including to determine whether those transactions or activities appear suspicious:
    - They are complex,
    - Unusually large,
    - Conducted in an unusual pattern, and/or
    - They do not have an apparent economic or lawful purpose.

The Firm does not knowingly/actively accord support to illegal activities.

4.6.10 Cryptoassets

A recognised definition of cryptoasset is: 'A digital representation of value that is not issued or guaranteed by a central bank or a public authority, is not necessarily attached to a legally established currency and does not possess a legal status of currency or money, but is accepted by natural or legal persons, as a means of exchange, and which can be transferred, stored and traded electronically.'

Certain cryptoasset businesses are in scope of the MLRs 2017 (as amended), which means that they will be subject to the requirements of the MLRs, including to have policies, controls and procedures in place to manage ML and CTF risks, but also to register with the appropriate AML supervisor – the FCA.

The FCA has published a webpage explaining different aspects of the cryptoasset regime, including its registration process, supervisory approach and change in control requirements.

As highlighted by numerous bodies (including the FCA, FATF, G20) the main risks from cryptoassets are to: financial crime prevention, consumers and market integrity. There is also the potential for issues in cryptoasset markets to transfer to other markets.

FATF reports that virtual currencies are vulnerable to money laundering, terrorist and proliferation financing and provide for the circumvention of sanctions because they:

- Avoid the formal financial system.
- Allow greater anonymity than traditional payment methods.
- Make tracing more difficult.
- Can be traded on the internet with relative ease anywhere in the world with/through third parties that may not have any (obvious) physical real-world presence – this also exposes users to internet trading hacking risk.
- Generally involve non-face-to-face relationships.
- Have the potential to permit anonymous funding, including third-party funding through virtual exchanges that do not properly identify the source of funds.
- Have the potential to permit anonymous transfers if due diligence on sender and receiver is inadequate.
- Remain largely outside the scope of regulation in many jurisdictions, although virtual asset service providers (VASPs) are in scope of the MLRs in the UK and in many other jurisdictions.
- The absence of, or differences in, regulation and oversight means markets are exposed to traditional forms of manipulation and abuse.

Currently the main financial crime impacts for the Firm and its ARs from cryptoassets are where:

- An investor's source of funds/wealth is, or involves, cryptoassets – conduct risk-based due diligence taking into account the weak audit trail and the potential for cryptoassets to be used for, or to launder proceeds from, illicit activity.
- An investment is recommended in a cryptoassets firm – conduct risk-based due diligence, initially and on an ongoing basis (where the risk is considered high), including on the founders. As more jurisdictions publish their regulatory position on cryptoasset products and services, checking the regulatory status of firms involved in cryptoasset activities, and their degree of compliance with relevant rules, is essential.

Although investments in cryptoassets have been increasing as investors seek better potential returns than more traditional investments, cryptoassets activity remains relatively low in comparison to more traditional/main-stream forms of investment. Therefore, the Firm considers its risk from cryptoassets to be low. However, it has noted that the involvement of large businesses is increasing the popularity/use of cryptoassets, therefore, it will keep this risk assessment under review as the sector develops.

Where the Firm or an AR are considering becoming involved in cryptoassets space, the following best practice principles should be considered and implemented:

- Developing staff knowledge and expertise on cryptoassets to help them identify the clients or activities which pose a high risk of financial crime.
- Ensuring that existing financial crime frameworks adequately reflect the crypto-related activities which the Firm is involved in, and that they are capable of keeping pace with fast-moving developments.
- Understanding the control and ownership structures of cryptoasset firms before establishing a business relationship or conducting an occasional transaction.
- Engaging with clients to understand the nature of their businesses and the risks they pose.
- Carrying out due diligence on key individuals in the client business including consideration of any adverse intelligence.
- In relation to clients offering forms of crypto-exchange services, assessing the adequacy of those clients' own due diligence arrangements.
- For clients which are involved in initial coin offerings, considering the issuer's investor-base, organisers, the functionality of tokens (including intended use) and the jurisdiction.

4.6.11 Unexplained Wealth Orders

UWOs are orders issued by the High Court, subject to certain conditions – see below – being met, to authorised officers of appropriate supervisory authorities (e.g. FCA, NCA and HMRC) requiring the respondent to provide a statement that sets out the nature and extent of their interest in the property covered by the order, and requiring them to explain how they obtained the property. Where trustees of a settlement hold the property, the UWO may require details of the settlement. The explanation must include details of how any costs incurred in obtaining the property were met.

The UWO will set out the form and manner in which the statement should be given, whom it should be given to and where it is to be given or sent. It may be accompanied by a request to provide information or documents.

An agency applying for a UWO must apply to the court specifying or describing the property for which it is seeking the order and the person it thinks holds the property. UWOs are able to capture persons and property outside the UK.

The court will make the UWO if it is satisfied:

- The respondent holds the property and it is worth more than £50,000.
- There are reasonable grounds to suspect the respondent's known sources of legitimate income would not have been sufficient to enable the respondent to acquire the property.
- There are reasonable grounds for suspecting that the property has been obtained through unlawful conduct.
- The respondent is either a PEP, or family member/known close associate of a PEP, 'responsible officers' of the entity that owns the property, or there are reasonable grounds to suspect the respondent/someone connected to the respondent, is or has been involved in a serious crime anywhere in the world.

When applying to the court for a UWO, the relevant enforcement authority may apply at the same time for an interim freezing order which would prohibit the person receiving the UWO from selling it.

If the respondent fails (without a reasonable excuse) to comply with the UWO's requirements in the specified timeframe, then the property will become 'recoverable property' for the purposes of POCA.

It will be a criminal offence to knowingly or recklessly make a misleading statement when responding to a UWO and could be punishable by up to 2 years' imprisonment and/or an unlimited fine.

4.6.12 Interim Freezing Orders

POCA allows the High Court to make an interim freezing order in respect of any property that is the subject of a UWO, on the application of the relevant enforcement authority, if it thinks there is a risk a recovery order resulting from the UWO might otherwise be frustrated. Once made, the enforcement authority can apply for a receiver to be appointed.

4.7 Financial Sanctions

Financial sanctions are restrictions put in place by the UK government that limit the provision of certain financial services, or restrict access to financial markets, funds and economic resources, in order to achieve a specific foreign policy or national security objective. The Sanctions and Anti-Money Laundering Act 2018 (the Sanctions Act) provides the legal framework for the UK to impose, update and lift sanctions autonomously.

FATF recommendations target proliferation financing, as well as ML and TF, and require countries to implement targeted financial sanctions to comply with UN Security Council resolutions and also to criminalise the act. The UK's Counter Proliferation programme can be viewed here.

Financial sanctions come in many forms but the most common types of financial sanctions currently in use or used in recent years are:

- Targeted asset freezes, which are usually applied to named individuals, entities and bodies, restricting access to funds and economic resources.
- Restrictions on a wide variety of financial markets and services – these can apply to named individuals, entities and bodies, to specified groups or to entire sectors. To date these have taken the form of: investment bans; restrictions on access to capital markets; directions to cease banking relationships and activities; requirements to notify or seek authorisation prior to certain payments being made or received; and restrictions on provision of financial, insurance, brokering, advisory services or other financial assistance.
- Directions to cease all business of a specified type with a specific person, group, sector or country.

The Office of Financial Sanctions Implementation (OFSI, part of HMT) helps to ensure that financial sanctions are properly understood, implemented, and enforced in the UK. The Economic Crime (Transparency and Enforcement) Act 2022 has strengthened OFSI's powers.

All firms are required to comply with the UK's sanctions regime completely. Dealing with individuals/entities subject to sanctions is a criminal offence. The OFSI can also impose civil monetary penalties and publish details of breaches that have not resulted in a monetary penalty.

All clients, individuals and entities should be screened against the sanctions list as part of initial and ongoing KYC due diligence and evidence of screening should be placed on file. The lists are available here. If screening results in a match the Firm's Compliance Officer or MLRO should be notified and their instructions followed.

Specific exemptions or licencing grounds exist to enable certain future transactions to take place that would otherwise be prohibited. Licences can only be issued by OFSI (Office of Financial Sanctions Implementation) and it may attach conditions to licences. Licences cannot be issued retrospectively.

The most up-to-date version of the legislation that imposes a specific sanctions regime must always be referred to. These can be found here.

Staff within the Firm and ARs are advised to sign up to OFSI alerts. This can be done here.

For more information on sanctions, visit the OFSI website.

4.8 Bribery and Corruption

4.8.1 Introduction

In general terms, bribery is defined as giving someone a financial or other advantage to encourage that person to perform their functions or activities improperly, or to reward that person for having already done so. Therefore this could cover seeking to influence a decision-maker by giving some kind of extra benefit to that person rather than by what can legitimately be offered as part of a tender process.

Transparency International (TI), a global organisation that works with governments, businesses and citizens to tackle corruption, defines corruption as 'The abuse of entrusted power for private gain.' TI explains that corruption can be further classified, according to the amounts of money lost and the sector in which it occurs, as:

- Grand corruption: 'Consists of acts committed at a high level of government that distort policies or the central functioning of the state, enabling leaders to benefit at the expense of the public good.'
- Petty corruption: 'Everyday abuse of entrusted power by low- and mid-level public officials in their interactions with ordinary citizens, who often are trying to access basic goods or services.'
- Political corruption: is the 'Manipulation of policies, institutions and rules of procedure in the allocation of resources and financing by political decision makers, who abuse their position to sustain their power, status and wealth.'

TI's website contains further information on corruption, including animated definitions of key terms in its Anti-Corruption Glossary.

The Bribery Act 2010, together with the Criminal Finances Act 2017 (see below), provides the legal framework to combat bribery and corruption. In the UK government's Anti-Corruption Strategy 2017-2022, the government outlines its continued commitment to making sure the UK financial sector, and the financial sectors of its Overseas Territories and Crown Dependencies, remain hostile to illicit finances.

The Bribery Act 2010 establishes 4 categories of offence:

1. Bribing another person (active bribery).
2. Being bribed (passive bribery).
3. Bribing a foreign public official.
4. Failure of a commercial organisation to prevent bribery on its behalf.

The first 3 offences are capable of being committed by an individual or a company but only a company can commit the fourth offence.

The Ministry of Justice has published Guidance for firms on how to prevent bribery by persons associated with them. Associated persons include agents, representatives, contract workers and some suppliers, as well as staff members.

A possible defence against the corporate offence of failing to prevent bribery is having effective measures in place to prevent bribery. These measures should be: risk based and proportionate; owned by senior

management; effectively communicated to staff and associated persons; and regularly monitored and reviewed.

ARs have the same exposure as the Firm under the Act for failing to prevent bribery by associated persons.

4.8.2 Anti-Bribery and Corruption Policy

The Firm operates a zero-tolerance approach to bribery and corruption and has an anti-bribery and corruption (ABC) policy in place (see Appendix L), which all members of staff and ARs are required to read, understand and comply with, and all other associated persons need to be aware of.

4.8.3 Anti-Bribery and Corruption Risk Assessment

The Firm's clients are typically UK-incorporated limited companies and UK-based LLPs, which are registered as ARs with the FCA. The ownership structure of its clients tends to be quite flat/non-complex and rarely involve individuals outside of the senior management. Where an AR is an LLP with a corporate partner, the directors/owners of the corporate partner are fully established.

It is noted that companies and limited partnerships (LPs), especially Scottish LPs, are particularly attractive to criminals due to the relative ease and low cost way in which they can be incorporated and dissolved, and that they are subject to few reporting and transparency obligations than other corporate forms .

To date none of the Firm's ARs are LPs. A number of funds managed by the Firm are structured as LPs but the Firm, as manager but also as principal for the fund advisers (ARs) is significantly involved in the set up and oversight of the funds. In addition, none of the Firm's ARs have been owned or controlled by a PEP or an organisation linked to a PEP.

The Firm only accepts introductions from known contacts and conducts thorough checks on prospective clients and their senior management regardless of the source of the referral, in accordance with its risk-based approach.

The Firm conducts enhanced due diligence in situations of higher risk and has strict guidelines, including a low approval threshold, for gifts and hospitality.

The Firm receives monthly reports on activities from its ARs and conducts a full routine monitoring visit at least every 12 months.

As such, the Firm considers its ABC risk to be low to moderate.

4.8.4 ABC Controls

The Firm has adopted the following controls to prevent bribery taking place – ARs should have similar controls in place:

- Clear, documented responsibility for reducing the risk of financial crime, including bribery and corruption. This responsibility rests with both the MLRO and Compliance Officer.
- Senior management understand and are informed of the bribery and corruption risks facing the Firm via the provision of management information addressing the financial crime risk.
- Senior management are required to review and approve, in advance, all higher risk relationships (such as those linked to a PEP or known close associate of a PEP).
- Remuneration structures are designed to avoid incentivising staff to gain business through bribes.
- Regular reviews of risk management by senior management which include the Firm's exposure to financial crime risk and the systems and controls in place to mitigate this risk.

- Risk-based approval for third-party payments and documentation demonstrating a clear understanding of the reason behind all payments.
- Where necessary, monitoring of any schedule of third-party payments (large payments, a large number of small payments, payments to connected parties, payments to political connections, high-risk jurisdictions, unusual, complex or secret payments).
- Countries regarded as higher risk in terms of bribery and corruption in accordance with the Transparency International Corruption Perception Index factored into risk assessments.
- Prohibiting provision of cash to staff (apart from de minimis amounts to cover small incidental expenses on an exceptional basis).
- Policy on gifts and incentives – see section 7 and Appendix L.
- Prohibition on the receipt or giving of cash gifts.
- Performing checks when recruiting new staff that are proportionate to their respective roles, e.g. criminal record checks.
- Providing staff with relevant, understandable and effective training.

4.9 Tax Evasion Facilitation

4.9.1 Introduction

The Criminal Finances Act 2017 (CFA) came into force on 30/09/17 and, amongst other things, comprises 4 parts:

- Part 1 – deals with proceeds of crime, money laundering, civil recovery, enforcement powers and related offences. It also creates a range of new powers for law enforcement agencies.
- Part 2 – ensures relevant money laundering and asset recovery powers will be extended to investigations under the Terrorism Act 2000 and the Proceeds of Crime Act (POCA) 2002.
- Part 3 – creates 2 new corporate offences of failure to prevent facilitation of tax evasion in the UK or abroad.
- Part 4 – contains minor and consequential amendments to POCA and other legislation.

The CFA follows on from the UK government's Action Plan for AML and CTF and key provisions are detailed below.

1.9.2 Corporate Failure to Prevent Tax Evasion

The CFA, amongst other things, contains 'failure to prevent' offences, similar to that in the Bribery Act 2010, in relation to tax evasion facilitation:

- Failure to prevent facilitation of UK tax evasion covers any offence of cheating the public revenue and any other fraudulent evasion of tax, thereby including duty and VAT fraud.
- Failure to prevent facilitation of foreign tax evasion captures conduct by an associated person that:
    - Amounts to an offence under foreign law.
    - Relates to a breach of duty relating to tax imposed under the law of that country.
    - Would be regarded by the courts of any part of the UK as amounting to being knowingly concerned in, or in taking steps with a view to, the fraudulent evasion of that tax.

Facilitation offences include aiding, abetting and inchoate offences (e.g. incitement).

As with the corporate offence under the Bribery Act, the new CFA offences are on a legal entity basis. Therefore, **ARs have the same exposure as the Firm under the Act for failing to prevent the facilitation of tax evasion by associated persons**.

The following 3 stages apply to both offences and each stage must be satisfied:

- Criminal tax evasion by a taxpayer (either an individual or a legal entity) under existing law.
- Criminal facilitation of the tax evasion by an 'associated person' of the relevant body acting in that capacity.
- Failure of the relevant body to prevent its representative from committing the criminal facilitation act.

It should be noted that there is no requirement for the Firm to have benefitted from the facilitation to commit the offence.

The offences cover all 'relevant bodies', including bodies corporate and partnerships, **wherever** formed, but not natural persons.

A person is 'associated' with a relevant body if that person is a staff member, agent or other person who performs services for or on behalf of the relevant body. The question as to whether a person is performing services for or on behalf of an organisation is intended to be broad in scope and is determined by reference to all the relevant circumstances. Therefore associated persons are likely to include: staff members at all levels, directors, officers, agency workers, seconded workers, volunteers, interns, agents, contractors, external consultants, third-party representatives and business partners.

For the corporate offence to be committed there must be criminal facilitation of the taxpayer by a person acting in the capacity of a person associated with the relevant body (stage 2). The associated person must deliberately and dishonestly take action to facilitate the taxpayer-level evasion. The UK offence does not radically alter what is criminal; it simply focuses on who is held to account for acts contrary to current criminal law.

Additional requirements apply to the foreign offence, as it is narrower in that only relevant bodes with a UK nexus can commit it and 'dual criminality' applies – where there are equivalent offences at both the taxpayer and associated person facilitation levels in the relevant overseas jurisdiction and the actions of both the taxpayer and facilitator would be offences under UK law.

HMRC has produced guidance to assist firms in the prevention of tax evasion. The guidance states the following, which helps explain the scope of the new law relating to the new offences:

'The legislation aims to tackle crimes committed by those who act for or on behalf of a relevant body. The legislation does not hold relevant bodies to account for the crimes of their customers, nor does it require them to prevent their customers from committing tax evasion. Nor is the legislation designed to capture the misuse of legitimate products and services that are provided to customers in good faith, where the individual adviser and relevant body did not know that its products were intended to be used for tax evasion purposes.'

The Act provides firms with a defence that if, at the time the offence was committed, they had in place 'A system of reasonable procedures that identified and mitigated tax evasion facilitation risks, then prosecution is unlikely.' (Source: HMRC Guidance)

As with the Bribery Act guidance, the CFA guidance is centred around 6 principles/key actions:

1. Conduct a risk assessment.
2. Implement proportional risk-based procedures.
3. Obtain and demonstrate top-level commitment form.
4. Conduct sufficient due diligence.
5. Communicate the Firm's approach and procedures, including from senior management and through appropriate training.
6. Monitor and review the Firm's policy and relevant procedures at least annually.

The guidance also contains illustrative examples of the different types of procedures that would be relevant for various types of companies. For example, timely self-reporting will be viewed as an indicator that a relevant body has reasonable procedures in place.

The penalties for facilitating tax evasion will include unlimited financial penalties and ancillary orders such as confiscation orders.

The key considerations for senior managers of corporate entities are as follows:

- What are my responsibilities under the new legislation?
- How can I discharge them?
- How are procedures implemented and documented?
- How often are they tested?

1.9.2.1 Risk Assessment

The Firm typically has no more than 15 limited companies incorporated in the UK and/or UK-based LLPs that are registered as ARs with the FCA. Directors and partners of ARs are required to be FCA Approved Persons. ARs and their Approved Persons are therefore required to be fit and proper for the duration of their relationship with the Firm and for as long as they hold Approved Person status.

The Firm and its ARs are only able to deal with Professional Clients and Eligible Counterparties, which can include high net worth individuals classed as Elective Professional Clients.

For a small number of fund clients the Firm also acts as the AIFM or delegated sub-manager. In these situations the Firm's responsibilities include approving fund subscriptions.

At any time the Firm's associated persons may include the following – those marked with an asterisk are considered potential sources of tax evasion facilitation risk:

- Individuals approved as CF30s under the Firm or Certified staff at Firm level.*
- Other staff members, partners or agents of the Firm or its ARs.*
- Gem Compliance Consulting Ltd (Gem) and staff members/agents of Gem.*
- Its accounting firm.*
- Its legal advisers.*
- Back-office function providers, including: (virtual) office space providers; Dropbox (cloud-based file storage provider); Office 365; IT consultants; online training platform(s); newsletter platform.
- Third-party professional connections (entities and individuals) that occasionally provide business referrals to the Firm on an informal, zero-remuneration basis.

Although the Firm operates in the financial services sector, which is considered by HMRC as a higher risk sector in respect of tax evasion, for the following reasons the Firm believes the risk that an associated person could facilitate tax evasion is low-medium:

- Its typical clients (ARs) are seen as relatively low risk from a financial crime perspective.
- Activities on its behalf are conducted predominantly in the UK and non-UK activity is largely within relatively low-risk jurisdictions.
- The Firm uses reputable businesses that undertake to comply with, inter alia, strict codes of practice, and their staff are required to maintain their competence in many areas including financial crime.
- The Firm's lawyers and accountants, whilst potentially higher risk associated persons, are firms covered by their own professional regulation, including their own financial compliance regimes.
- The transactions the Firm is directly involved in are not overly complex and are considered sufficiently transparent.
- The parties involved in the transactions are well known to the Firm.

- It has appropriate agreements in place with all clients and associated persons (with the exception of those that make informal business referrals to the Firm).
- Third-party business referrals to the Firm are from well-known contacts and no reliance is placed on any due diligence conducted by, or assurances from, the introducer. (See standard AR selection procedure for more information.)
- The senior management of its clients are all Approved Persons subject to the FCA's FIT criteria – see earlier section for a description of this.
- The FCA's Principles for Businesses apply to the Firm and its ARs.
- Fund clients use well-known, reputable firms, which are subject to the same/equivalent financial crime regulations/legislation as the Firm, to assist them in structuring and administering the funds, including conducting detailed KYC on underlying investors, which in some cases the Firm is required to approve beforehand.

Although the risk is seen as low-medium the potential risk that does exist primarily stems from the Firm's ARs and Approved Persons, as they are seen as an extension of the Firm for regulated activities, and Gem, which operates many of its back-office processes, including AR and Approved Person pre-application due diligence.

4.9.2.2 Risk Mitigation

- Robust AR selection and onboarding procedures.
- On the Firm's behalf, and in accordance with the Firm's operational procedures, Gem conducts extensive pre-application due diligence on prospective ARs and their senior management teams before submitting applications to the FCA for appointment/approval.
- Clear and regular AR training programme, which includes financial crime training and covers the CFA specifically.
- Issuance of relevant ad hoc guidance to ARs covering topics such as incentives and performance management.
- Clear zero-tolerance policy on tax evasion prevention, which has been approved and communicated to all clients and associated persons of the Firm by the Firm's Managing Partner.
- Other relevant policies and procedures include those relating to:
    - AML, CTF and CPF, risk-based due diligence in particular.
    - Gifts, benefits and hospitality.
    - Fraud.
    - Remuneration.
    - Whistleblowing.
- Request details of the CFA policies/stance of associated persons, where applicable, as part of the Firm's initial due diligence.
- Relevant clauses in terms and conditions, including contracts for services, service agreements, and subscription agreements – require natural and legal persons to take all relevant steps to prevent the facilitation of tax evasion.
- Template KYC and client categorisation checklist contains:
    - Zero-tolerance statement.
    - Requirement to conduct tax-related due diligence.
- Allocation of responsibility for ensuring front-line compliance with the procedures by clients to one of the Firm's partners (Kevin Gallacher).
- Proportionate scrutiny of bank details for payments to/from clients, associated persons and underlying investors.
- Where structures include an overseas element the rationale for this should be checked and documented. Where the rationale is tax-related documentary evidence confirming the legitimacy

of the structuring, and compliance with relevant laws, from appropriately qualified persons is required.

4.9.2.3 Red Flags and High-Risk Indicators

Higher risk situations and possible signs of tax evasion are similar to those for fraud, and AML/CTF, so AML/CTF processes and procedures are relevant to preventing/spotting tax evasion. Other possible signs include:

- Overly complex company structure(s) covering a number of jurisdictions without sufficient supporting information to justify the structure(s).
- Difficulty in establishing UBOs and reluctance to provide requested information.
- A lifestyle (as evidenced from internet searches and social media) that is not commensurate to the declared income and wider information provided to date.
- Difficulty in establishing source of wealth and/or funds.
- Payments made to/from third-party accounts with no obvious, or at best a tenuous, connection to the individual/entity.
- Failure to provide details of their registration with HMRC's Affluent Unit (for those subject to UK revenue and customs laws and with net wealth of between £2.5m and £20m).
- Unusual activity on bank statements that could be suggestive of 'off the book' deals.
- Multiple transactions of buying and selling within a Group between subsidiaries and often across jurisdictions, including known tax havens (see list below), without a clear commercial reason for operating such a complex model.

HMRC has published a report outlining the use of tax avoidance schemes in the UK, which can be accessed here.

See also Part 1 of the JMLSG Guidance, which can be accessed here, for high-risk factors that can also apply to tax fraud – Annex 1 – jurisdictions, and Annex II – Customers.

According to a news report, the following jurisdictions are the biggest enablers of global corporate tax abuse:

- The Cayman Islands
- British Virgin Islands
- Bermuda
- Luxembourg
- Netherlands
- Hong Kong
- Singapore
- United Arab Emirates
- Jersey
- Switzerland

The background and purpose of all complex and unusually large transactions, and all unusual patterns of transactions, which have no apparent economic or lawful purpose should be examined as far as is reasonably possible.

If a member of staff becomes suspicious, they should send a SAR along with all relevant supporting documentation, to the Firm's MLRO without delay. The staff member should ensure they do not alert the subject to the filing of a report and await further instructions from the MLRO before proceeding further.