MAINFIRST

ANTI-MONEY LAUNDERING & COUNTER-TERRORIST FINANCING POLICY

MAINFIRST AFFILIATED FUND MANAGERS (DEUTSCHLAND) GMBH

11.2024

Version 9.0

Anti-Money Laundering & Counter-Terrorist Financing Policy

Content

MainFirst Affiliated Fund Managers (Deutschland) GmbH (hereinafter the “Company”) is required to establish and maintain effective systems and controls to prevent the risk that might be used for financial crime and to have an adequate risk management framework in place as well as policies and procedures aiming at the prevention of money laundering, terrorist financing and further criminal acts that might put the Company’s assets at risk or that are directed against third parties (e.g. clients).

The object of this AML & CTF Policy is to implement the statutory and regulatory provisions on combating money laundering and preventing the financing of terrorism, which are laid down in the German Money Laundering Act (Geldwäschegesetz - “GWG”) and the Law on Supervision of Securities Institutions (Gesetz zur Beaufsichtigung von Wertpapierinstituten – “WpIG”) as well as the Act on the Enforcement of Economic Sanctions (Sanctions Enforcement Act,

Sanktionsdurchsetzungsgesetz - SanktDG). It sets out the internal rules and principles, as well as related actions, which the Company must implement in order to comply with the following obligations:

1. Obligation to perform AML and KYC due diligence procedures
2. Obligation to monitor on a permanent basis and pay special attention to certain activities and transactions engaged by the Company (on its own account or on behalf of the Funds)
3. Obligation to keep certain records and information
4. Obligation to have an adequate internal organization to address the AML and CTF purpose
5. Obligation to cooperate with the authorities

Employees of the Company shall be sensitized to the problem of money laundering in order to limit the risk that the Company or its employees are unintentionally misused for the "laundering" of illegally acquired assets or for the financing of a terrorist organization. Acts or transactions that are suspected of serving money laundering or terrorist financing must therefore be rejected as a matter of principle, without prejudice to the other obligations explained below.

This Policy applies to the Company and to all permanent and short-term employees including governing bodies of the Company, secondees, external consultants, contractors and agency employees while they are at the Company. It provides for companywide minimum standards to ensure compliance with statutory rules and best industry practice.

It considers the Company’s business model according to which:

a. Operations are largely based in European Economic Area (EEA) jurisdictions and Switzerland
b. The business focus is on investment and ancillary services to eligible counterparties and professional clients and on relevant activities
c. Emphasis is given on EEA markets and listed instruments and products
d. As a matter of policy, no services are provided to individuals (no retail, private banking or wealth management),
e. As a standard rule, the Company does not offer any deposits, provide payment services to clients, open or maintain payable-through accounts and carry out occasional transactions other than as part of a business relationship.

This Policy is available for all employees of the Company via the corporate Intranet. Regular monitoring, auditing and evaluation ensure continuing relevance.

The Company has sufficient internal guidelines and rules applying the national legislation and regulation relating to the German Anti Money Laundering Act and especially implement the

conditions set by § 6 Par. (2) no. 1 GWG.

The Company's internal control organisation regarding the prevention of money laundering and the compliance with the AML and CFT obligations follows **the three lines of defence** model. Responsibility for compliance with the AML and CTF Framework lies with Management

The Company is responsible for ensuring compliance with this Policy in their area of responsibility at entity or business level respectively. As required by law, Management oversees all AML and CFT efforts, has established an AML and CTF program comprising policies, procedures, internal controls and systems including customer and third party Due Diligence (CDD), suspicious transaction identification and reporting, ensures staff training and awareness and that recording and retention requirements are complied with. It enforces the standards and takes appropriate corrective action when weaknesses or compliance failures are identified.

The internal audit function is the third line of defence in the internal control organisation, which provides for independent review of the processes established and - if performed - do random controls of individual controls or events. The Company's internal audit function assesses the AML and CTF framework on an annual basis. As mandated by German law, external auditors as independent third party assess AML and CTF policies and practices and report on the Company's AML and CTF systems and controls including identified weaknesses and findings on an annual basis to Management and the German regulator, whereby additional stand-alone external audit requirements may apply in other jurisdictions. There are no relevant IT systems and interfaces in use. This Policy is valid for each employee of the Company.

1 Definitions

a) Money Laundering

Money laundering is the process by which proceeds from a criminal activity are disguised to conceal their illicit origins in order to "legitimize" the ill-gotten gains of crime. Criminal property may take any form, including money or money's worth, securities, tangible property and intangible property. The term also includes money used to finance terrorism; however it comes about.

Money laundering activity includes:

a. The conversion or transfer of property, knowing that such property is derived from criminal activity or from an act of participation in such activity, for the purpose of concealing or disguising the illicit origin of the property or of assisting any person who is involved in the commission of such activity to evade the legal consequences of that person's action.
b. The concealment or disguise of the true nature, source, location, disposition, movement, rights with respect to ownership of property, knowing that such property is derived from criminal activity or from an act of participation in such activity.
c. The acquisition, possession or use of property, knowing, at the time of receipt, that such property was derived from criminal activity or from an act of participation in such activity.
d. Participation in, association to commit, attempts to commit and aiding, abetting, facilitating and counselling the commission of any of the actions mentioned in the foregoing points. Predicate acts are defined pursuant to national criminal law and generally include fraud, embezzlement, theft, misappropriation, robbery, insider trading, market manipulation, corruption, bribery and tax-related crimes.

Money laundering is a single process. However, the money laundering cycle can be broken down into three distinct stages:

1. The **placement** stage where proceeds of crime are entered into the financial system.
2. The **layering** stage involving the structuring of complex financial transactions that obscure the audit trail.
3. The **integration** stage where criminal proceeds are fully integrated into the financial system and can be used for any purpose.

b) Terrorist Financing

Pursuant to Section 1 (2) of the GWG, terrorist financing is

- the provision or collection of assets with the knowledge or the intention that these assets will be used, in whole or in part, to commit one or more of the following offences:
  - founding, supporting or recruiting members or supporters for a terrorist organization in Germany or abroad (= offenses under Sections 129a and 129b of the Criminal Code – Strafgesetzbuch StGB); or
  - any other of the offences described in Articles 3, 5 to 10 and 12 of Directive (EU) 2017/541 of the European Parliament and of the Council of 15 March 2017 on combating terrorism and replacing Council Framework Decision 2002/475/JHA and amending Council Decision 2005/671/JHA[1].
- the commission of a terrorist offense under Section 89c of the Criminal Code: financing of a terrorist offense committed with the aim of seriously intimidating the population, unlawfully coercing public authorities or an international organization by force or threat of force, or seriously destroying or seriously impairing the basic political, constitutional, economic or social structures of a country or an international organization; by the nature of its commission or its effects, the offense must be capable of seriously damaging a state or an international organization.

Pursuant to Section 129a of the German Criminal Code, a terrorist organization is an organization whose purposes or activities are directed toward the commission of criminal acts punishable by a maximum term of imprisonment of at least two years.

c) Financial Crime / White-collar crime

All wilful criminal acts committed in any jurisdiction in which the Company offers its services in any way that

- affect the bottom line: financial crime against the Company that could lead to a significant deterioration of the Company's business or standing including in case of operational loss with direct impact on assets, earnings and reputation or
- where third parties suffer (financial crime e.g., fraud against clients).

[1] Direct terrorist offenses, offenses related to a terrorist organization, public provocation to commit a terrorist offense, recruitment for terrorist purposes, conducting training for terrorist purposes, completing training for terrorist purposes, traveling for terrorist purposes, organizing or facilitating travel for terrorist purposes, financing terrorism, as well as grand larceny, extortion, and the preparation of forged administrative documents in support of terrorist offenses.

Such intentional criminal acts could be

- external criminal acts: these are circumstances where the Company business or standing might be seriously endangered and/or third parties might suffer serious operational and/or reputational damage due to criminal acts by a third party (e.g., client, broker, counterparty, supplier) or
- internal criminal acts: circumstances where at least one internal party participates in the commission of the crime (e.g., employee).

By way of example and without prejudice to national rules, such acts comprise fraud, embezzlement/ misappropriation, theft, robbery and robbery by blackmail, other white collar crime criminal offences aiming at protecting the general interest in business and public administration (e.g. check and credit card fraud, investment fraud), corruption including bribery and accepting an advantage, insolvency offences, tax-related crimes, aiding and abetting, criminal acts against the free competition, data espionage and unlawful interception of data, identity theft.

2 Framework

The Company applies a series of preventive measures with a view to prevent money laundering and terrorist financing. The means by which any controls must be performed will depend on the assessment, which the Company has to make of the Money Laundering (ML) and Terrorist Financing (TF) risk of each customer relationship, so called “Risk Based Approach”.

3 Policy Statement and Top-Level Commitment (“Tone at the Top”)

The Company makes every effort to remain in full compliance with applicable anti-money laundering laws, rules and standards in the jurisdictions in which the Company does business. Moreover, the Company is committed to full compliance with embargos and financial sanctions in the jurisdictions in which it operates.

4 Internal Organisation, Safeguards & Internal Controls

4.1 Internal Policies and Procedures

The Company has established adequate and appropriate written policies and procedures of customer and third-party due diligence, reporting, record keeping, internal control, risk assessment, risk management, compliance management and communication of such policies and procedures to forestall and prevent operations related to money laundering or terrorist financing.

4.2 Internal Safeguards

The company takes appropriate measures as well as updates and monitors appropriate business and customer-related security systems to prevent money laundering, the financing of terrorism and other criminal acts at the expense of the Company. The focus is on a risk-oriented approach. The systems and measures must consider the individual size, organisation and risk situation of the respective institution.

The internal security measures essentially consist of the following points:

a) appointment of a money laundering officer (GwB) directly subordinated to the management. The money laundering officer is responsible for compliance with money laundering regulations; the responsibility of the management level remains unaffected. The money laundering officer is directly subordinate to the management.
b) developing and updating internal policies, appropriate business and customer related safeguards and controls to prevent money laundering and terrorist financing. The Company has taken adequate measures to prevent and detect financial crime against the Company, including its employees and clients and enforce compliance with applicable rules. Such measures further include staff awareness i. e. ensuring that employees have access to up-to-date information on relevant legal and regulatory developments and changes to existing AML/CTF related policies, the practices of money launderers and terrorist financers and on indications leading to the recognition of suspicious transactions.
c) ensure that employees involved in conducting transactions and initiating and establishing business relationships are informed of money laundering and terrorist financing methods and obligations under the Money Laundering Act
These measures include participation of all employees in induction training upon commencement of employment with or assignment to the Company as well as ad-hoc and annual training programs to help employees recognize operations which may be related to money laundering or terrorist financing and to instruct them as to how to proceed in such cases, inform them of internal policies to prevent money laundering and terrorist financing and provide examples of different forms of money laundering involving Company products and services.
d) regular, risk-oriented checks on the reliability of employees.

In the event of employment of third parties to carry out some the AML/CTF relevant functions, the Company ensures that such parties receive proper AML/CTF training that includes identification and reporting of transactions that must be reported to government authorities, examples of different forms of money laundering involving Company products and services and internal policies to prevent money laundering.

4.3 Internal Controls

The nature and extent of the Company's systems and controls depends on a variety of factors, including the degree of risk associated with each area of operation, the nature, scale and complexity of the business, the type of products, clients, and activities involved, the diversity of operations, including geographical diversity, the volume and size of transactions, and the distribution channels. Systems of internal control include the identification of senior management responsibilities, the provision of regular and timely information to senior management on money laundering and terrorist financing risks, the training of relevant employees on the legal and regulatory responsibilities, money laundering and terrorist financing controls and measures, the documentation of the business' AML/CTF risk management policies and procedures as well as measures to ensure that money laundering and terrorist financing risks are taken into account in the day-to-day operation of the business.

4.4 Customer and Third-Party Due Diligence (CDD)

The Company applies CDD measures

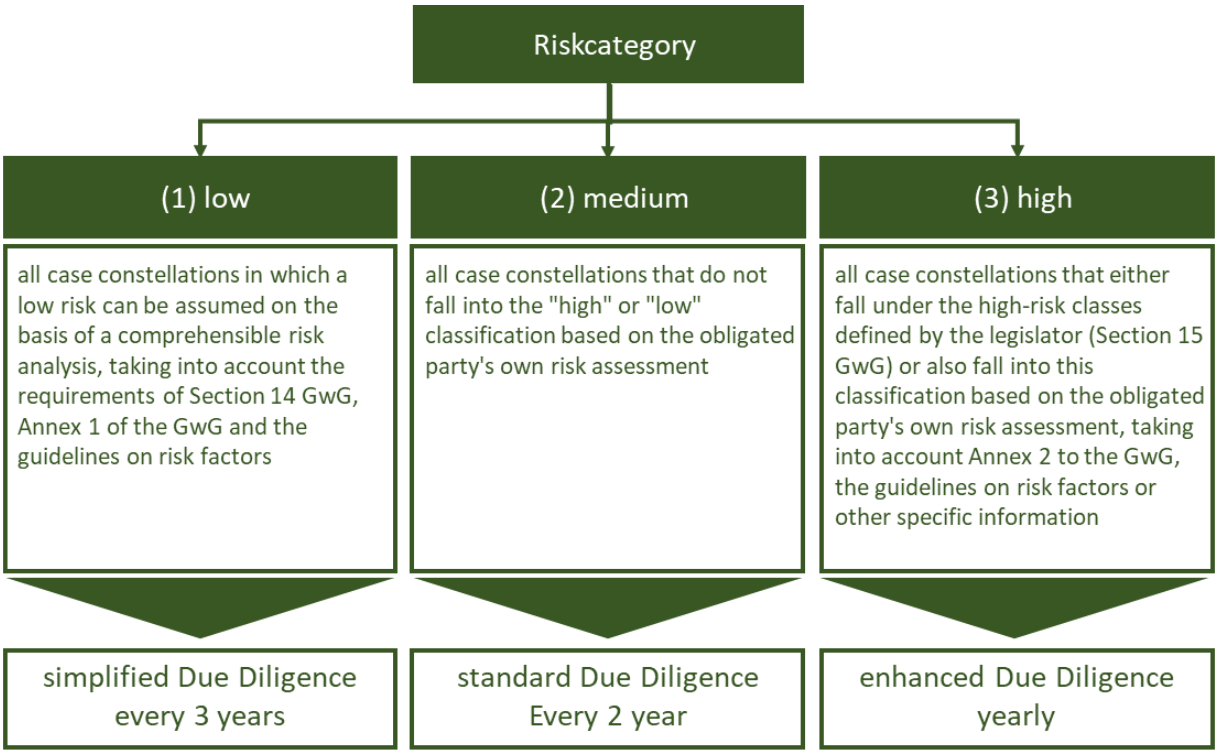
a) when establishing a business relationship with a client or business partner,
b) when there is a suspicion of money laundering or terrorist financing, regardless of any derogation, exemption, or threshold and
c) when there are doubts about the veracity or adequacy of previously obtained client identification data.

The Company does not execute transactions or money transfers outside of established business relationships.

Customer Due Diligence measures ("Know Your Customer" (KYC)) imply:

i. The identification of the client/business partner and identity verification.
ii. The identification of beneficial owner, where applicable, and taking risk-based and adequate measures to verify the identity so that the Company is satisfied that it knows who the beneficial owner is, including, as regards legal persons, trusts and similar legal arrangements, taking risk-based and adequate measures to understand the ownership and control structure of the client/business partner.
iii. Obtaining information on the purpose and intended nature of the business relationship.
iv. Conducting on-going monitoring of the business relationship including scrutiny of transactions undertaken throughout the course of that relationship to ensure that the transactions being conducted are consistent with the Company's knowledge of the client, the business and risk profile as well as ensuring that the documents, data or information held are kept up to date. CDD measures are adapted depending on the risk classification annually to every 3 years (**risk-based approach**). Clients and third parties are classified as low, medium or high risk according to set risk factors. Three levels of due diligence are hereby defined on a risk-sensitive basis depending on the identified AML risk: Simplified, Standard and Enhanced Due Diligence.
v. Ad hoc vigilance towards relationships involving particular risks.

The following chart illustrates the different risk categories:



Whenever entering into a new business relationship, the Company shall perform, as the case may be with the assistance of the AML/ CTF Officer and of the nominees, the evaluation of the ML/TF risk rating of each customer/business partner, such assessment is notably done on the basis of the following criteria (not exhaustive):

i. Country of nationality/origin/incorporation;
ii. Country of residence/registered office;
iii. Profession/Industry/activities performed;
iv. Politically Exposed Person (PEP) status;
v. Remote business relationship;
vi. Any other criteria that the Compliance Officer may deem appropriate from time to time.

The Company shall ensure that the outcome of the evaluation is properly documented. Should the outcome of the evaluation show a higher risk of money laundering or terrorist financing, then **Enhanced Due Diligence (EDD)** must apply. In other situations, the Company may conclude on the fact that the business relationship involves very limited risks of money laundering or terrorist financing. In this latter case, the Company may decide to apply a **Simplified Due Diligence Process (SDD**).

The Company must apply ***enhanced customer due diligence*** in situations which by their nature or otherwise according to its own judgement, can present a higher risk of money laundering or terrorist financing.

The **EDD** will notably cover the following situations (non-exhaustive list):

- the customer or beneficial owner is a politically exposed person (PEP), a family member, or a person known to be a close relative pursuant to Section 1 (12) sentence 2 No. 12a to l and No. 2 GwG

- it is a business relationship or a transaction involving a high-risk third country or a natural or legal person resident in such a third country (e.g. Customers and intermediaries involved in the fund distribution from high-risk countries)
- it is a transaction that, compared to similar cases,
  - is particularly complex or unusually large
  - follow an unusual transaction pattern; or
  - occurs without an obvious economic or legitimate purpose
  - products, structures or transactions that favour anonymity (such as bearer shares)
  - intermediaries subscribing fund units on behalf of underlying customers (nominees)
  - use of complex distribution channels
- it is a cross-border correspondent relationship with respondents domiciled in a third country or, subject to an assessment by the Company as higher risk, in a country of the European Economic Area
- the profession and the business sector of the customer are considered as high risk[2]

Simplified Due Diligence measures can be applied under the following conditions:

- The counterparty is a listed company whose securities are admitted to trading on a regulated market in a country recognized as equivalent; or
- The counterparty is an institution (e.g. credit or financial institution) supervised by the local supervisor in an EU country or regulated in a country considered as equivalent; or
- The customer is an EU member state public authority or body.

The Company must ensure that it obtains with the assistance or through the AML/CTF Officer, sufficient information from the customer in order to confirm that it falls under one of the above-mentioned categories.

The Company must perform with the assistance or through the AML/CTF Officer the regular review of such customer in order to ensure that the categorization remains relevant for each customer.

Should any suspicion arise on a customer in due course, then EDD must be applied, and the level of risk of the customer updated accordingly.

If the Company is unable to comply with applicable CDD obligations, it may **not establish** a business relationship or carry out the transaction or shall terminate the business relationship and shall consider making a report to the Financial Intelligence Unit (FIU) and the office of the district attorney.

In the case of agency or outsourcing relationships on a contractual basis between the Company and external natural or legal persons that are not subject to any anti-money laundering and terrorist financing rules, any anti-money laundering and anti-terrorist financing obligations for those agents or outsourcing service providers as part of the Company, shall be provided for in

[2] This includes, but is not limited to: handles large amount of physical cash (e.g. casinos, clubs), money service business (e.g. bureaux de change), gaming and gambling businesses, computer, high-tech, telecom or mobile phone sales and distribution or distributors, military consultants and companies involved primary in either arms manufacture or sales, individuals or companies whose operations lead to environmental damage/pollution, individuals and companies involved in adult entertainment, time share companies, correspondent banks, companies operating or dealing with virtual currencies.

the agency, outsourcing or other contracts with such parties. The same applies in case of reliance on third parties for the performance of certain CDD obligations as permitted by national law. The reason is that the responsibility for complying with applicable rules remains with the Company.

5 Embargos and Financial Sanctions Compliance Program

The Company has implemented a risk-based compliance program reasonably designed to comply with the different embargo and financial sanctions requirements in the jurisdictions the Company operates. The Company considers applicable financial sanctions and embargos based on United Nations (UN) Resolutions, European Union (EU) Regulations, national, or other sources. Hereby asset freezes imposed by statute or directly applicable by EU Regulations are applied. Under the relevant legislation it is a criminal offence for any natural or legal person to:

a) Deal with the funds of designated persons
b) Make funds, economic resources or financial services available, directly or indirectly, to designated persons or to make funds available to another person for the designated person's benefit
c) Participate knowingly and intentionally in activities the object or effect of which is (directly or indirectly) to circumvent a prohibition or enable or facilitate the contravention of any such prohibition without doing so under the authority of a license issued by competent national authorities.

"Deal with" means:

- In respect of funds: use, alter, move, allow access to or transfer or deal with, in any other way that would result in any change in volume, amount, location, ownership, possession, character or destination, or make any other change that would enable use, including portfolio management, and
- In respect of economic resources: use to obtain funds, goods or services in any way, including (but not limited to) by selling, hiring or mortgaging the resources.

The Company has appropriate policies and procedures in place to monitor transactions to prevent breaches of the financial sanctions legislation. In particular, client data is scanned against relevant embargo and financial sanctions lists.

6 Company and Employee Suspicious Activity Reporting Obligations

According to § 43 GwG, the Company is required to file a suspicious activity report without undue delay to the national Financial Intelligence Units (FIUs), where the Company knows, suspects or has reasonable grounds to suspect that money laundering or terrorist financing is being or has been committed or attempted, regardless of the value of the asset or the transaction amount.

The Company is required to furnish the competent FIU with all necessary information, in accordance with applicable rules.

Employees shall thus pay special attention to any activity which they regard as particularly likely, by its nature, to be related to money laundering or terrorist financing and in particular complex or unusually large transactions and all unusual patterns of transactions which have no apparent economic or visible lawful purpose.[3]

Employees shall report any suspicious transactions to their AML Officer responsible and/or Management without undue delay. Concerned transactions shall, as a matter of principle, not be carried out before filing the report with the competent FIU. By way of derogation from the general prohibition on executing suspicious transactions, the Company upon prior informed consultation with and express approval by the AML Officer may execute suspicious transactions before informing the competent authorities, where refraining from the execution thereof is impossible or likely to frustrate efforts to pursue the beneficiaries of a suspected money laundering or terrorist financing operation, in which case the FIU or office of the district attorney shall be informed immediately afterwards. This, however, shall be without prejudice to any further obligations under the applicable counter-terrorist financing rules.

Employees shall not disclose to the customer concerned or to other third persons the fact that information has been transmitted for suspicious transaction reporting purposes or that a money laundering or terrorist financing investigation is being or may be carried out (tipping-off prohibition) except where authorized under applicable rules. Employees making suspicious reports on money laundering or terrorist financing grounds are protected from threat and hostile action. If a suspicious activity report was filed to the competent authorities. They will be informed about this.

7 Record Keeping

8

The Company retains documents and information for use in any investigation into, or analysis of, possible money laundering or terrorist financing by the FIU or by other competent authorities in accordance with national law:

a) In the case of CDD, a copy or the references of the evidence required, for a period of at least five years after the business relationship with their customer has ended.
b) In the case of business relationships and transactions, the supporting evidence and records consisting of the original documents or copies admissible in court proceedings under the applicable national legislation for a period of at least five years following the carrying-out of the transactions or the end of the business relationship.

The Company has effective systems in place which are commensurate with the size and nature of its business that enable the Company to reply fully and within an appropriate timeframe to enquiries from FIUs or other authorities as to whether they maintain or have maintained during the previous five years a business relationship with specified persons and on the nature of the relationship.

[3] See **Appendix 1** for a non-exhaustive list of suspicious transaction indicators.

9 Enforcement

The Company supervises employee compliance with the rules described in this Policy. Employees shall be held liable for infringements of applicable rules leading up to immediate termination of employment. In case of suspicion of employee involvement in suspicious activity notification duties to the competent authorities may additionally apply.

10 The Company's Financial Crime Prevention Framework

The Company's approach for managing financial crime risk can be summarized as follows.

10.1 Policy Statement: Company Ethics

The Company is committed to achieving the highest standards of ethical conduct and complying with applicable laws and regulations. The Company takes a zero-tolerance approach to financial crime including corruption, bribery and fraud and is committed to upholding applicable laws and regulations in relation to countering financial crime. Considering applicable rules in the different jurisdictions it operates, the Company regularly evaluates its procedures for preventing financial crime so as to ensure they remain effective.

10.2 Governance: Top Level Commitment

The Management is committed to AML and Financial Crime Prevention procedures. They take clear responsibility for managing financial crime risks including combatting corruption, bribery and fraud and are actively engaged in the approach to addressing relevant risks. Management Information in terms of regular and ad hoc reporting and briefings ensure proper escalation and up-to-date knowledge of relevant financial crime issues.

10.3 Structure: Internal Organization, Roles and Responsibilities

The Company's internal control organisation regarding the prevention of financial crime and compliance with relevant obligations follows the three lines of defence model. Responsibility for compliance with the Financial Crime Prevention Framework lies with Management.

Management:

The Company and Business Management are responsible for ensuring compliance with this Policy in their area of responsibility at entity or business level respectively. As required by law, the Management has appointed a Chief Financial Crime Prevention and AML Officer and local officers to oversee the Company's efforts in this field, has established a Financial Crime Prevention Program comprising policies, procedures, internal controls and systems (e-mail: verdachtsmeldung@mainfirst.com) including on CDD and on internal whistleblowing (e-mail: whistleblowing@mainfirst.com), ensures staff training and awareness and that recording and retention requirements are complied with. It enforces the standards and takes appropriate corrective action when weaknesses or compliance failures are identified.

Business Staff (1st Level Control) (e.g. Front Office, Operations, IT, HR):
Vigilant business control staff are key to the Company's Financial Crime Prevention Policy regarding client and third-party acceptance and on-going transactions and activity monitoring for the detection and prevention of financial crime. Their role is supplemented by manual or IT controls and solutions as deemed necessary for compliance with applicable rules.

The Financial Crime Prevention (FCP) Officer (2nd Level Control):

This is the function responsible for the oversight of the Company's compliance with applicable financial crime prevention rules. Considering that counter-fraud and AML efforts can complement each other this is a combined function with the AML/CTF Office. The Company has appointed an AML/FCP Officer. The AML/FCP Officer is responsible for relevant internal control and compliance management. The AML/FCP Officer reports at least annually and ad-hoc to the Management and the owner and is responsible for:

a) The definition and update of internal policies and procedures
b) The on-going development of adequate strategies to prevent the misuse of new products and technologies that could facilitate the anonymity of business relationships and transactions
c) Conducting and updating, as necessary, an entity and group-wide risk assessment for Financial Crime Prevention purposes including but not limited to bribery and corruption risk-based on which risks resulting from such internal or external criminal acts or omissions are identified, assessed and relevant actions recommended and taken
d) Ensuring that there is a coordinated approach vis-à-vis the annual AML/CTF risk assessment
e) Advising on measures to be taken, in particular for internal security purposes including monitoring and control measures resulting from the annual risk identification and assessment exercise
f) Reviewing the adequacy and effectiveness of controls and control systems in place
g) Creating clear and coordinated reporting lines and relevant reporting duties
h) Serving as key point of contact for law enforcement agencies and regulatory authorities in financial crime compliance matters.

The internal and/or external audit functions (3rd Level Control):

This is the third line of defence in the internal control organisation which provides for independent review of the processes established and - if performed - do random controls of individual controls or events. The internal audit function assesses the Financial Crime Prevention Framework (policies, procedures, systems and controls) on an annual basis.

Moreover, in accordance with German law, external auditors as independent third party assess AML/FCP policies and practices and report on the Company's AML/FCP systems and controls including identified weaknesses and findings on an annual basis to Management and the German regulator, whereby additional stand-alone external audit requirements may apply in other jurisdictions.

10.4 Risk Assessment

The Company undertakes an assessment of financial crime risks including but not limited to fraud, corruption and bribery across the organization. The objective is to achieve a thorough understanding of financial crime risks to apply appropriate systems and controls. Risk assessment is a continuous process based on information available from internal and external

sources. Hereby both the impact of financial crime risk on MainFirst and on clients is considered. Relevant risk factors are:

i. Country risk,
ii. Sectoral risk,
iii. Product risk,
iv. Transaction risk,
v. Client and third-party risk (business opportunity and business partnership risk),
vi. Distribution channel risk
vii. Other, as deemed appropriate under the circumstances

10.5 Policies and Procedures: The Company's Financial Crime Prevention

The Company has implemented guidelines and controls to fight financial crime including corruption, bribery and fraud as mandated by applicable laws and regulations.

10.6 Staff Recruitment, Vetting, Training, Awareness and Remuneration

The Company employs staff who possess the skills, knowledge, and expertise to carry out their functions effectively. Employee competence is reviewed regularly, at least annually, by responsible Management and appropriate action is taken to ensure they remain competent for their role. Vetting and training are appropriate to employee roles. Hereby the financial crime risk to which staff is exposed is considered. All staff is subject to background checks including submission of a certificate of good conduct by competent local authorities in the course of the recruiting process and prior to employment and at intervals during employment with the Company depending on the financial crime risk they face. Where employment agencies are used, the Company periodically ensures that they adhere to the agreed vetting standard. All staff undergoes a reliability review by responsible Management on an annual basis. Furthermore, every employee has to obtain and deliver an excerpt of the criminal record to HR. Additionally, every employee receives induction and annual financial crime prevention training. Staff remuneration rules ensure that staff is not rewarded for taking unacceptable financial crime risks. Any changes in policy and procedures or new developments are communicated on an on- going basis to Management and relevant staff by the AML & FCP Officer and responsible Management.

10.7 Internal Whistleblowing Procedure

Employees have the right and are encouraged to disclose to the AML & FCP Officer in good faith any information which in the reasonable belief of the reporting employee, tends to show that a financial crime has been committed, is being committed or is likely to be committed or that any relevant matter has been, is being or is likely to be deliberately concealed, where the employee has reason not to discuss such matters with the responsible Management. Such a reason could be a suspected Management involvement in or knowledge of such criminal acts or any suspected Management non-action in case of employee speak-up or any other reason the employee might have not to use the standard Management reporting and escalation process.

The purpose of this is financial crime detection, prevention, and enforcement to best protect the Company including its employees and clients. It is immaterial where the relevant failure occurred or is likely to occur and which law is applicable. Reasonable suspicion suffices. Employees are not

expected to initiate stand-alone investigations or report facts. However, reporting should not be based on mere rumours.

The AML & FCP Officer shall acknowledge and assess the disclosure, determine whether it falls within the internal whistleblowing rules and inform accordingly the reporting employee within five working days upon receipt of the filled-out reporting form (Appendix 2 or 3). In the affirmative, the FCP Officer shall treat such protected disclosures with utmost confidentiality and not disclose the identity of the reporting employee to any parties involved in such reporting without the reporting employee`s consent. In case there is a legal, regulatory, or other duty to disclose the situation to any external authorities, then the AML & FCP Officer shall inform the reporting employee accordingly, unless not permitted under applicable rules. In such cases, the Company shall offer the employee any necessary support. The AML & FCP Officer shall then assess whether any further reviews or investigations are necessary and initiate any further action as needed.

The AML & FCP Officer may request the support of other independent departments (e. g. internal audit) or coordinate things with external parties (e.g., external counsel) as deemed necessary.

In case of a direct disclosure to the AML & FCP Officer and unless the employee has a reasonable objection to the report being forwarded to the AML & FCP Officer of the respective entity of employment, the FCP Officer will inform the Management thereof. The AML & FCP Officer working on the case will inform the reporting employee of the negative outcome of the review. If upon review the AML & FCP Officer has reasonable grounds for suspicion that criminal acts have been or are likely to be committed or concealed, then the AML & FCP Officer shall promptly inform responsible Management and advice on further action to be taken. Upon Management decision on appropriate action, the AML & FCP Officer shall inform the reporting employee accordingly. The AML & FCP Officer keeps a confidential internal whistleblowing log to assess effectiveness of the policy and any emerging trends and reports regularly on an anonymous basis to responsible Management.

The Company ensures that the reporting employee will not be subjected to any detriment by any act, or any deliberate failure to act, by the Company done on the ground that the employee has made a protected disclosure including non-fulfilment of the employment contract or termination of employment (non-retaliation-protection).

Non-retaliation-protection and support of the employee in any proceedings by competent authorities does not apply where the employee is involved in the criminal act. However, in such case employees are encouraged to report their reasonable suspicion of such acts being or to be committed or concealed considering any impact of such self-reporting in the course of any resulting court or other proceeding.

If in the course of the review it turns out that the employee reported the situation at issue in bad faith, HR will be notified accordingly.

10.8 Quality of Oversight: Monitoring and Review

The Financial Crime Prevention Framework is subject to regular review to ensure that financial crime policies, systems and controls remain effective. The Company maintains monitoring arrangements tailored to its activities and size in accordance with local legal and regulatory requirements and best practice.

Internal audit and the Financial Crime Prevention Officer routinely test the Company’s defences against financial crime, including specific financial crime threats whereby the allocation of audit and FCP Officer Resources is risk-based. Management engages constructively with processes of oversight and challenge.

11 Escalation

If the described policy leads to inconsistencies or problems, the following defined escalation chain must be adhered to.

First escalation level	Policy Owner
Second escalation level	Head of Department (if different from the first escalation level)
Third escalation level	Management
Fourth escalation level	Shareholders

In the case of compliance-relevant topics, Legal & Compliance must also be informed immediately.

12 Appendix

Appendix 1: How to recognize potential suspicious activity

This is an indicative list of indicators that a transaction might be suspicious. Depending on the circumstances these factors could result in grounds for suspicion or the need for further scrutiny:

a) At the outset of a business relationship - prior to contracting and account opening

- The CDD process (identification and verification) is uncommonly difficult, or the prospect does not cooperate (e.g., refuses disclosure of ultimate beneficial owner or does not provide the company‘s family tree where needed)
- There appears to be inconsistencies in the information provided by the customer
- The supporting documentation does not add validity to the other information provided by the client
- The customer is in a hurry to rush a transaction through, with promises to provide the information later
- The prospect is seated in a high-risk country
- There are several risk-increasing factors e.g. prior criminal convictions; the capacity of the prospect as a politically exposed person who may be at risk of exposure to corruption; the prospect is in a business with high levels of cash income that could lend itself to money laundering by mixing criminal cash with legitimate takings; the prospect sets up shell companies with nominee shareholders and/or directors whereby use of nominees is excessive or unnecessary; has companies with capital in the form of bearer shares; the prospect operates in countries with lax AML controls or with high levels of organized crime, corruption or from which terrorist organizations are known to operate; there are frequent changes to shareholders or directors; the company accounts are not up-to-date; purchase of companies with no obvious commercial purpose; subsidiaries with no apparent purpose or companies which continuously make substantial losses or uneconomic group structures for tax purposes
- The prospects want to conduct cash transactions, wishes physical delivery of securities or make an unusual request for collection or delivery
- The explanation for the business and/or the amounts involved are not credible
- The prospect is represented by third parties (proxy representation through lawyers, notary public, auditors) or intermediaries who are not subject to adequate anti-money

laundering laws; no face-to-face meeting with the prospect takes place for non-plausible reasons
- Transactions having no apparent purpose or which make no obvious financial sense, or which seem to involve unnecessary complexity e.g. the prospect seeks to establish a business relationship with a MAINFIRST entity without reasonable justification where the same service may be offered to the prospect in the country of residence or transaction execution at a much lower price, with less complications and more efficiently
- Unnecessary routing of funds through third parties

b) Client activity - transaction execution and settlement

- There seems to be no economic reason for the transactions, they are not settled directly but through deviations and leave clients with a loss; the identity of participating parties remains unclear
- Financial instruments should be delivered not via the usual clearing and settlement institutions, transactions should take place by way of physical delivery of financial instruments. Effective financial instruments are delivered by the client or through an unknown institution
- A series of small buy transactions in an instrument type and transfers from other institutions are sold as one position. The price is not paid in the usual currency/in the usual account or should be paid out in cash
- Credits in financial instruments or account is transferred to third parties who do not have an apparent relationship with the client and are seated in high-risk countries
- Upon client instruction, transactions should be settled at non-market prices
- The settlement instructions (standing delivery/payment instructions) are being changed repeatedly without apparent reason and last-minute
- The transaction is different from the normal business of the customer or unusual for the type of business. The size or frequency of the transaction is not consistent with the normal activities of the customer. There are sudden increases in the frequency/value of transactions of a particular customer without reasonable explanation
- Use of bank accounts in several currencies without reason, transfers of funds without underlying transactions, unexplained transfers of significant sums through several bank accounts

c) Examples of activity that might suggest to staff that there could be potential terrorist activity

- Embargo or financial sanctions listing for client or relevant person (e.g. Management, shareholders, ultimate beneficial owner) e.g. via world-check “hit”
- Frequent address changes
- Media reports e.g. on suspected or arrested terrorists or groups

Appendix 2: Internal Suspicious Transaction Reporting Form to the AML officer

- 0012_Internal_Suspicious_Transaction_Reporting_Form

Appendix 3: Internal Whistleblowing Reporting Form

- 0012_Internal_Whistleblowing_Reporting_Form