MAINFIRST

MAINFIRST GROUP ANTI-MONEY LAUNDERING, COUNTER-TERRORIST FINANCING

Applicable to	MainFirst Group
Scope:	Global
Applicable as of:	January 3, 2018
Version:	4.0
MainFirst document hierarchy:	A 9
Author:	Compliance

MAINFIRST

Table of Contents

1 Introduction

MainFirst Bank AG, its subsidiaries and affiliates (collectively "MainFirst") is required to establish and maintain effective systems and controls to prevent the risk that it might be used to 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 MainFirst assets at risk or that are directed against third parties (e.g. clients). Operating in a cross-border context within and outside the EU, MainFirst is called to develop group policies and a consolidated group approach as part of global risk management to ensure compliance with existing legislation and regulation, as well as with internal policies and ethical standards.

2 Scope and Purpose

This Policy applies to MainFirst Bank AG, its subsidiaries and affiliates and to all permanent and short-term Employees including secondees, external consultants, contractors and agency Employees while they are at MainFirst. It provides for firm-wide minimum standards to ensure compliance with statutory rules and best industry practice. It considers the MainFirst Business Model according to which (a) MainFirst operations are largely based in EEA jurisdictions, Switzerland and the USA; (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, MainFirst does not offer any deposits, does not provide payment services to clients, does not open or maintain payable-through accounts and does not carry out occasional transactions other than as part of a business relationship. MainFirst Entities should adopt or retain higher standards or stricter rules in local implementing policy if so required under local law. However, in case of conflict between local law and the minimum requirements under this Policy, especially where local legislation in this area is deficient, this Policy shall prevail. This Policy is available on the intranet. Regular monitoring, auditing and evaluation ensure continuing relevance.

3 Definitions

3.1. What is 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. It also covers money, however come by, which is used to fund terrorism.

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.[1] 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

and

(3) the integration stage where criminal proceeds are fully integrated into the financial system and can be used for any purpose.

3.2. What is Terrorist Financing?

Terrorist financing is the financing of terrorist acts, and of terrorists and terrorist organizations. Financing means the provision or collection of funds, by any means, directly or indirectly, with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out terrorist

[1] National law applies (Sec. 1 para. 1 Anti Money Laundering Act, Sec 261 German Criminal Code). This is the definition according to the 4th AML Directive. E.g. in the UK a stricter definition of money laundering is in place (i.e. no intention to launder money required, suspicion is sufficient for a principal money laundering offence, conversion or transfer of criminal property suffices, relevant for the proceeds of all crime not only serious crime, there are no de minimis provisions, see Sections 327, 328, 329 and 340 in the Proceeds of Crime Act 2002).

offences, offences related to a terrorist group, offences linked to terrorist activities, inciting, aiding or abetting, and attempting an offence[2].

3.3. What is Financial Crime?

All wilful criminal acts committed in any jurisdiction MainFirst offers its services in any way that (a) affect the bottom line: financial crime against MainFirst that could lead to a significant deterioration of MainFirst business or standing including in case of operational loss with direct impact on assets, earnings and reputation or (b) where third parties suffer (financial crime e.g. fraud against clients).

Such intentional criminal acts could be (a) external criminal acts: these are circumstances where MainFirst 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, other) or (b) 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, theft, misappropriation, 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.

4 MainFirst AML/CTF Framework

MainFirst applies a series of preventive measures with a view to prevent money laundering and terrorist financing:

4.1. Policy Statement and Top Level Commitment (“Tone at the Top”)

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

4.2. Internal Organization, Internal Controls and Communication

4.2.1. Internal Controls

The nature and extent of MainFirst 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

[2] National law applies (Sec. 1 para. 2 Anti Money Laundering Act). This is the definition according to the 4th AML Directive. For further details on the different terrorist financing offences, see Articles 1 to 4
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
.

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.

4.2.2. Internal Organization. Roles and Responsibilities

The MainFirst internal control organization regarding the prevention of money laundering and the compliance with the AML/CTF obligations follows the three lines of defence model. Responsibility for compliance with the AML/CTF Framework lies with Management.

Management: MainFirst Entity 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, Management has appointed a Chief AML/CTF Officer and local AML/CTF Officers to oversee MainFirst's AML/CTF efforts, has established an AML/CTF program comprising policies, procedures, internal controls and systems including on Customer and Third Party Due Diligence (CDD) and on 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 Front Office and Operational staff (1nd Level Control): Vigilant front office and operations staff are key to MainFirst AML/CTF policy regarding client and third party acceptance and on-going monitoring for the identification of suspicious activity. Their role is supplemented by manual or IT controls and solutions as deemed necessary for AML/CTF compliance.

The AML/CTF Officer (2nd Level Control): This is the function responsible for the oversight of MainFirst compliance with applicable AML/CTF rules. MainFirst has appointed AML Officers in each jurisdiction where the group operates, if so required, whereby the Group AML/CTF Officer is responsible at group level for relevant internal control and compliance management (advisory, policies, risk assessment, monitoring & control, annual and ad hoc Management and Supervisory Board reporting, staff training & awareness, processing and reporting suspicious transactions to competent authorities as well as interfacing with law enforcement generally).

The internal and external audit functions (3rd Level Control): This is the third leg in the internal control organization which provides for independent review and test controls after the event. The MainFirst Bank AG and MainFirst Schweiz AG internal audit function assesses the AML/CTF Framework on an annual basis. As mandated by German law, external auditors as independent third party assess AML/CTF policies and practices and report on the MainFirst AML/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.

4.3. Internal Policies and Procedures

MainFirst has established adequate and appropriate written policies and procedures of customer and third party due diligence[3], reporting, record keeping[4], internal control, risk assessment[5], risk management, compliance management and communication of such policies and procedures in order to forestall and prevent operations related to money laundering or terrorist financing. Further relevant policies and procedures include:

(a) Procedure on Identification and Reporting of Suspicious Transactions Objective is to enable Employees to identify and scrutinize complex or unusually large transactions, unusual patterns of transactions which have no apparent economic or visible lawful purpose and any other activity which could be considered to be related to money laundering or terrorist financing; further to define the AML/CTF Officer as the individual responsible to receive suspicious transaction reporting and relevant disclosures under applicable law , ensure employees report suspicious activity to the nominated AML Officer, and ensure the nominated AML Officer considers such internal reports in the light of available information and determines whether they give rise to knowledge or suspicion or reasonable grounds for knowledge or suspicion of money laundering or terrorist financing.

(b) Change Management Process including with respect to new products and markets, changes in business processes and structures and mergers & acquisitions6. This is to ensure among others that additional measures are specified and taken to prevent the use of products and transactions that favour anonymity for money laundering or terrorist financing or that entail an increased money-laundering or terrorist financing risk

(c) Policy on No Use of Cash or Physical Delivery of Financial Instruments[7]. Considering that the use of large cash payments or physical delivery of securities has repeatedly proven to be very vulnerable to money laundering and terrorist financing, MainFirst prohibits cash payments and physical delivery of securities.

(d) Policy on No Use of Shell Banks. For the same reason MainFirst prohibits the use of shell-banks (no accounts, no relationship, no transactions, products or business with, on behalf or for the benefit of shell banks) by MainFirst and by MainFirst correspondent banks.

(e) Policy on Correspondent Banking Dealings. MainFirst only deals with correspondent banks that possess licenses to operate in their countries of origin. Additional security and internal control measures are imposed to correspondent banking business to mitigate relevant risks.

(f) Policy on Client Onboarding,

[3] See below under 4.3.1. and the MainFirst Client and Counterparty Acceptance Policy
[4] See below under 4.4.
[5] The AML/CTF Officer conducts an annual AML/CTF Risk Assessment at group and entity level as mandated by national law
[6] See the MainFirst Group New Product Approval Policy
[7] See the MainFirst Group Anweisung Durchführung Tafelgeschäfte_Bartransaktionen Policy

(g) Employee Reliability Policy[8]. This is to ensure staff reliability under AML/CTF grounds

(h) Embargos and Financial Sanctions Compliance Program[9]

As part of effective compliance management arrangements, MainFirst carries out regular assessments of the adequacy of systems and controls to ensure that any money laundering and terrorist financing risks are effectively managed and that compliance with applicable rules is ensured. Appropriate monitoring processes and procedures have been established and are maintained in order to regularly review and test the effectiveness of relevant policies and procedures.

4.3.1. Customer and Third Party Due Diligence (CDD)

MainFirst applies CDD measures (a) when establishing a business relationship with a client, (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. MainFirst 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 and verification his/her identity; (ii) the identification of beneficial owner, where applicable, and taking risk-based and adequate measures to verify his/her identity so that MainFirst 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; (iii) obtaining information on the purpose and intended nature of the business relationship; and (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 MainFirst 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 perceived (risk-based approach). Clients and third parties are classified as low, medium or high risk according to set risk factors. Three levels of due diligences are hereby defined on a risk-sensitive basis depending on the identified AML risk: Simplified, Standard and Enhanced Due Diligence[10].

If MainFirst 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 MainFirst 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 MainFirst, shall be provided for in the agency, outsourcing or other contract with such parties. The same applies in

[8] See the MainFirst Group Policy on Employee Reliability
[9] See below under 4.3.2.
[10] For further details on the applicable CDD rules including enhanced customer due diligence for high-risk customers or business relationships, such as appropriate procedures to determine whether a person is a politically exposed person, and certain additional, more detailed requirements, such as the existence of compliance management procedures and policies, see the MainFirst Group Client and Counterparty Acceptance Policy.

case of reliance on third parties for the performance of certain CDD obligations as permitted by national law. Reason is that the responsibility for complying with applicable rules remains with MainFirst.

4.3.2. Embargos and Financial Sanctions Compliance Program

MainFirst has implemented a risk-based compliance program reasonably designed to comply with the different embargo and financial sanctions requirements in the jurisdictions MainFirst operates. MainFirst 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, or (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 (a) 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 (b) 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.

MainFirst has appropriate policies and procedures in place to monitor transactions in order to prevent breaches of the financial sanctions legislation: Employees take necessary steps to prevent dealings including but not limited to customer, broker and other counterparty account opening and transaction execution for, on behalf of, or for the benefit of, a sanctioned individual, entity, country or organization in violation of applicable sanctions regulations. The Operations Department considers the different international and domestic financial sanctions and embargos lists [11] and performs corporate security checks and/or further business controls in the course of Customer, Broker & Counterparty Due Diligence., in the course of a business relationship and with respect to transactions including payments according to internal procedures and upon relevant information by the AML Officer or directly by the OFAC in case of OFAC imposed economic sanctions. In particular, client data is scanned against relevant embargo and financial sanctions lists at the time an account is opened for a Brokerage client, at the commencement of a servicing relationship for all other clients, upon receipt of new client data or changes to existing client data, as well as upon updates to the applicable economic sanctions programs. In addition, and on a risk-based approach, payments are subject to six-eye-principle control and COO and/or Head of Finance sign-off[12] In the event of a "hit" e.g. that a prospect, client or third party is identified as a designated individual, entity, country or organization, Operations or Accounting & Control in case of payments, informs the AML Officer immediately and does not proceed with prospect onboarding, contract execution, the intended transaction until AML Officer written clearance is given, as this would be a breach of the financial sanctions rules. Additionally, in that case advice of competent authorities would need to be requested and a suspicious transaction reporting obligation to competent authorities might apply. MainFirst

[11] E.g. administered and enforced by the German Federal Bank, the French Ministry of Finance, the HM Treasury, the U.S. Department of the Treasury's Office of Foreign Assets Control (OFAC)
[12] See the MainFirst Accounting Guidelines

4.3.3. MainFirst and Employee Suspicious Activity Reporting Obligations

MainFirst is required to file a suspicious activity report promptly to the national financial intelligence units (FIUs) and the office of the district attorney of transactions or situations, where MainFirst knows, suspects or has reasonable grounds to suspect that money laundering or terrorist financing is being or has been committed or attempted. MainFirst is further required to furnish the competent FIU and office of the district attorney, at its request promptly, with all necessary information, in accordance with applicable rules[13].
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. See Appendix 1 for a non-exhaustive list of suspicious transaction indicators. Employees shall report any suspicious transactions to their responsible AML Officer without undue delay. Concerned transactions shall, as a matter of principle, not be carried out before filing the report with the competent FIU and office of the district attorney. By way of derogation from the general prohibition on executing suspicious transactions, MainFirst 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. [14]

4.4. Record Keeping

MainFirst 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[15]: (a) in the case of customer due diligence, a copy or the references of the evidence required, for a

[13] National law may provide for stricter rules e.g. French Law specifies the various cases of suspicious transactions reporting including cases of automatic STR without any prior individual internal analysis. Non automatic STR is provided for in case of sums or transactions suspected to be related to an offence sanctioned by more than 1 year imprisonment or related to terrorism financing, in case of sums or transactions suspected to be related to tax crimes if one the 16 criteria defined by Decree are met, as well as in case of unusual or complex transactions referred to in Article L.561-10-2 II of the Financial and Monetary Code. If the identity of the customer, or the beneficial owner, or the settler of a trust or any other equivalent structure remains doubtful, despite CDD vigilance, the law provides for an automatic STR duty. The same about transactions with persons in States or territories referred to in Article L.561-10 4° of the Financial and Monetary Code, i.e. designated States or territories whose legislation or business practices hinder the application of AML requirements.

[14] Group Compliance has a cross-supervisory approach to collaborate with MainFirst Bank's branches. This means that regulatory duties can be delegated to branch managers or representatives (e.g. for Italy SAR notification requirements as a delegated obligation to the local branch management).

[15] Sec. 8 para. 4 of the Anti Money Laundering Act provides for a period of at least 5 years (Note: implemented as such in DE, UK and FR AML Law). Where additional rules apply, MainFirst ensures adherence with national provisions. E.g. national law

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. MainFirst has effective systems in place which are commensurate with the size and nature of its business that enable MainFirst to reply fully and within appropriate timeframe to enquiries from FIUs or other authorities as to whether they maintain or have maintained during the previous 5 years a business relationship with specified persons and on the nature of the relationship.

4.5. Staff Awareness and Training

MainFirst takes appropriate measures so that relevant Employees are aware of the provisions in force. These measures include participation of all Employees in induction training upon commencement of employment with or assignment to MainFirst 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 MainFirst products and services[16]. 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. In case of employment of third parties to carry out some the AML/CTF relevant functions then MainFirst 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 MainFirst products and services and internal policies to prevent money laundering. Records of training sessions including attendance records and relevant training materials are retained.

4.6. Enforcement

MainFirst supervises Employee compliance with these rules. 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.

5 MainFirst Financial Crime Prevention Framework

MainFirst has taken adequate measures to prevent and detect financial crime against MainFirst including its Employees and MainFirst clients and enforce compliance with applicable rules. The MainFirst approach for managing financial crime risk can be summarized as follows:

may provide for longer retention periods e.g. Italian Legislative Decree 231/2007 sets out recording and retention requirements of ten years.

[16]For further details see the MainFirst Group Code of Conduct and the MainFirst Group Client and Counterparty Acceptance Policy

5.1. Policy Statement. MainFirst Ethics

MainFirst is committed to achieving the highest standards of ethical conduct and complying with applicable laws and regulations in the countries where MainFirst conducts business. MainFirst 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[17]. Taking into account applicable rules in the different jurisdictions it operates, MainFirst regularly evaluates its procedures for preventing financial crime so as to ensure they remain effective.

5.2. Governance: Top Level Commitment

The Board and Senior Management are committed to the MainFirst Financial Crime Prevention Program. 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. To this end, the Board of Management of MainFirst Bank AG has appointed an AML Officer at MainFirst Bank AG and group level and has adopted a relevant Policy Framework. 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.

5.3. Structure: Internal Organization. Roles and Responsibilities

The MainFirst internal control organization 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: MainFirst Entity 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, Management has appointed a Chief Financial Crime Prevention Officer and local Officers to oversee MainFirst's efforts in this field, has established an Financial Crime Prevention Program comprising policies, procedures, internal controls and systems including on Customer and Third Party Due Diligence (CDD) and on internal whistleblowing, 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 (1nd Level Control) (e.g. Front Office, Operations, IT,HR, Accounting & Controlling) : Vigilant business control staff are key to MainFirst Financial Crime Prevention policy regarding client and third party acceptance and on-going transaction 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 Officer (2nd Level Control): This is the function responsible for the oversight of MainFirst compliance with applicable financial crime prevention rules. Considering that counter-fraud and anti-money laundering efforts can complement each other this is a combined function with the AML/CTF Office. MainFirst has appointed AML /FCP Officers in each jurisdiction where the group operates, if so

[17] As mandated a.o. by Sec. 25h German Banking Act, Section 7 of the UK Bribery Act 2010 ("Failure to Prevent Bribery Offence") and Ministry of Justice Guidance, U.S. Foreign Corrupt Practices Act

required, whereby the Group FCP Officer is responsible at group level for relevant internal control and compliance management. The FCP Officer reports at least annually and ad hoc to the Board of Directors and the Supervisory Board 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, a MainFirst entity and group-wide risk assessment for Financial Crime Prevention purposes including but not limited to bribery and corruption risks on the basis of 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 external audit functions (3rd Level Control): This is the third leg in the internal control organization which provides for independent review and test controls after the event. The MainFirst internal audit function assesses the Financial Crime Prevention Framework (policies, procedures, systems and controls) on an annual basis. As mandated by German law, external auditors as independent third party assess FCP policies and practices and report on the MainFirst 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.

5.4. Risk Assessment

MainFirst 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 in order 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: country risk, sectoral risk, product risk, transaction risk, client and third party risk (business opportunity and business partnership risk), distribution channel risk and other, as deemed appropriate under the circumstances.

5.5. Policies and Procedures: MainFirst Financial Crime Prevention Program

MainFirst has implemented a compliance program to fight financial crime including corruption, bribery and fraud as mandated by applicable laws and regulations. The program is tailored to the group's specific needs, risks, and challenges. In particular, policies and procedures are proportionate to the risks MainFirst face as well as clear, practical and accessible to ensure that there is a practical and realistic means of achieving policy objectives across functions. They form part of the MainFirst Group Organizational Manual which is published prominently on the MainFirst intranet and is accessible to all Employees.

Hallmarks of the current program are:

(a) This Group Anti- Money laundering, Counter-Terrorist Financing and Financial Crime Prevention Policy.

(b) Change Management Process[18] including with respect to new products and markets, changes in business processes and structures and mergers & acquisitions. This is to ensure among others that financial crime risks are properly considered when designing new products and services.

(c) Prohibition of Facilitation Payments: MainFirst opposes any form of bribery, including facilitation payments, which are strictly prohibited across the organization.

(d) The Anti-Money Laundering Framework[19] in particular considering that certain criminal acts including bribery and corruption are predicate acts to money laundering offences.

(e) The Group Conflicts of Interest Management Policy and implementing rules on Management of personal conflicts in particular rules on Gifts and Entertainment, Outside Activities, Personal Account Dealing and Personal Investments[20].

(f) Customer and Third Party Due Diligence[21]: MainFirst applies due diligence procedures, taking a proportionate and risk based approach, in respect of persons who perform or will perform services for or on behalf of the organization, in order to mitigate identified financial crime including fraud and bribery risk. Clients, counterparties and third parties are formally accepted, pre-screened on corporate security grounds and are subject to on-going Due Diligence and Review.

(g) Staff Recruitment, Vetting, Training, Awareness and Remuneration Rules[22].

(h) Organizational Rules: segregation of duties (Sales/Sales Trading vs. Trading vs. Operations vs. Accounting & Controlling vs. Risk Management vs. Compliance), job rotation, clear reporting lines, clear proxy and signature rules, four eye principle, 10-days per year in one slot vacation rule (mandatory leave).

(i) The Group Whistleblowing Rules with respect to financial crime including fraud, corruption and offering or accepting bribes[23].

(j) Rules on Political or Charitable Contributions[24].

5.6. Staff Recruitment, Vetting, Training, Awareness and Remuneration

MainFirst employs staff who possesses the skills, knowledge and expertise to carry out their functions effectively. Employee competence is reviewed annually in the course of performance appraisal by responsible Management and appropriate action is taken to ensure they remain competent for their role.

[18] See the MainFirst Group New Product Approval Policy
[19] See Section 4 of this Policy
[20] See the MainFirst Group Conflicts of Interest Management Policy, the MainFirst Group Code of Conduct,_ MainFirst Personal Account Dealing Policy and the MainFirst Securities US Inc. Supervisory Procedures Manual
[21] See the MainFirst Group Client and Counterparty Acceptance Policy
[22] See below under 5.6.
[23] See below under 5.7. Employee concerns about commission of other wrongdoing, other conduct likely to harm the reputation of MainFirst or concerns relating to Employee personal circumstances at work are covered in relevant MainFirst policy.
[24] See the Gifts & Entertainment Policy in the MainFirst Group Code of Conduct

Vetting and training is appropriate to Employee roles. Hereby the financial crime risk to which staff is exposed is taken into account. In particular, 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 MainFirst depending on the financial crime risk they face. Where employment agencies are used, MainFirst periodically satisfies itself that they adhere to the agreed vetting standard. All staff undergoes a reliability review by responsible Management on an annual basis. Further 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[25]. Any changes in policy and procedures or new developments are communicated on an on-going basis to Management and relevant staff by the FCP Officer and responsible Management.

5.7. Internal Whistleblowing Procedure

Employees have the right and are encouraged to disclose to the Financial Crime Prevention Officer of their entity or directly to the Group Financial Crime Prevention 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 his/her responsible Management. Such 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.

Purpose is financial crime detection; prevention and enforcement to best protect MainFirst 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 FCP Officer shall acknowledge and assess the disclosure, determine whether it falls within the internal whistleblowing rules and inform accordingly the reporting Employee within 5 working days upon receipt of the filled out reporting form (Appendix 4). 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 FCP Officer shall inform the reporting Employee accordingly, unless not permitted under applicable rules. In such case MainFirst shall offer the Employee any necessary support. The FCP Officer shall then assess whether any further reviews or investigations are necessary and initiate any further action as needed. She/he 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 Group FCP Officer and unless the Employee has a reasonable objection to her/his reporting being forwarded to the FCP Officer of her/his entity of employment, the Group FCP Officer will inform the local FCP Officer thereof. Local FCP Officers shall inform the Group FCP Officer of any reporting under the internal whistleblowing system. The FCP Officer working on the case will inform the reporting Employee of the negative outcome of her/his review. If

[25] See also the MainFirst Annual Compensation Report

upon review the FCP Officer has reasonable grounds for suspicion that criminal acts have been or are likely to be committed or concealed then she/he shall promptly inform responsible Management and the COO and advise on further action to be taken. Upon Management decision on appropriate action, the FCP Officer shall inform the reporting Employee accordingly. The 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.

MainFirst ensures that the reporting Employee will not be subjected to any detriment by any act, or any deliberate failure to act, by MainFirst 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 turns out that the Employee reported the situation at issue in bad faith, HR will be notified accordingly.

5.8. 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. MainFirst 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 MainFirst 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.

6 Document History and Version Control

Version Number	Author	Date	Approval	Brief Description
1.0	Eleni Koulourioti	January 2014	Board of Management	Initial Document
2.0	Oliver Liszka	23.12.2015	Board of Management	Review and update
3.0	Andreas Kühnemund	31.01.2017	Board of Management	Review and update
4.0	Andreas Kühnemund	19.12.2017	Board of Management	Review and update

7 Appendices

Appendix 1: How to Recognize Potential Suspicious Activity
Appendix 2: MAINFIRST Bank AG Paris Branch: Additional Suspicious Transaction Reporting Obligations under French Law
Appendix 3: Employee Suspicious Transaction Reporting Form to the AML Officer
Appendix 4: Employee Internal Whistleblowing Reporting Form

Appendix 1

How to Recognize Potential Suspicious Activity

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

1. **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 familiy 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 wants to conduct cash transactions, wishes physical delivery of securities or makes 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 uses 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 MAINFIRSTentity without reasonable justification in particular where the same service may be offered to the Prospect in his/her country of residence or transaction execution at a much lower price, with less complications and more efficiently.
- Unnecessary routing of funds through third-parties.

2. 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 client 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.
- Credit 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

3. 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

MAINFIRST Bank AG Paris Branch
Lutte contre le blanchiment
Les obligations déclaratives

1. Que Déclarer?

(a) Les sommes inscrites dans leurs livres ou les opérations portant sur des sommes dont elles savent, soupçonnent ou ont de bonnes raisons de soupçonner qu'elles proviennent d'une infraction passible d'une peine privative de liberté supérieure à un an ou participent au financement du terrorisme (Article L561-15).
(b) Les sommes ou opérations dont ils savent, soupçonnent ou ont de bonnes raisons de soupçonner qu'elles proviennent d'une fraude fiscale lorsqu'il y a présence d'au moins un critère défini par le décret du 16/07/2009.
(c) Toute opération pour laquelle l'identité du donneur d'ordre ou du bénéficiaire effectif ou du constituant d'un fonds fiduciaire ou de tout autre instrument de gestion d'un patrimoine d'affectation reste douteuse
(d) Par décret: toute opération effectuée par un résident d'un pays à dispositif de LCB-FT insuffisant

2. Les déclarations de soupçon en cas de fraude fiscale (Décret n° 2009-874 du 16 juillet 2009)

Les sommes ou opérations dont les personnes assujettis savent, soupçonnent ou ont de bonnes raisons de soupçonner qu'elles proviennent d'une fraude fiscale lorsqu'il y a présence d'au moins un critère suivant:

1° L'utilisation de sociétés écran, dont l'activité n'est pas cohérente avec l'objet social ou ayant leur siège social dans un Etat ou un territoire qui n'a pas conclu avec la France une convention fiscale permettant l'accès aux informations bancaires, identifié à partir d'une liste publiée par l'administration fiscale, ou à l'adresse privée d'un des bénéficiaires de l'opération suspecte ou chez un domiciliataire;

2° La réalisation d'opérations financières par des sociétés dans lesquelles sont intervenus des changements statutaires fréquents non justifiés par la situation économique de l'entreprise ;

3° Le recours à l'interposition de personnes physiques n'intervenant qu'en apparence pour le compte de sociétés ou de particuliers impliqués dans des opérations financières ;

4° La réalisation d'opérations financières incohérentes au regard des activités habituelles de l'entreprise ou d'opérations suspectes dans des secteurs sensibles aux fraudes à la TVA de type carrousel, tels que les secteurs de l'informatique, de la téléphonie, du matériel électronique, du matériel électroménager, de la hi-fi et de la vidéo ;

5° La progression forte et inexpliquée, sur une courte période, des sommes créditées sur les comptes nouvellement ouverts ou jusque-là peu actifs ou inactifs, liée le cas échéant à une augmentation importante du nombre et du volume des opérations ou au recours à des sociétés en sommeil ou peu actives dans lesquelles ont pu intervenir des changements statutaires récents ;

6° La constatation d'anomalies dans les factures ou les bons de commande lorsqu'ils sont présentés comme justification des opérations financières, telles que l'absence du numéro d'immatriculation au registre du commerce et des sociétés, du numéro SIREN, du numéro de TVA, de numéro de facture, d'adresse ou de dates;

7° Le recours inexpliqué à des comptes utilisés comme des comptes de passage ou par lesquels transitent de multiples opérations tant au débit qu'au crédit, alors que les soldes des comptes sont souvent proches de zéro;

8° Le retrait fréquent d'espèces d'un compte professionnel ou leur dépôt sur un tel compte non justifié par le niveau ou la nature de l'activité économique;

9° La difficulté d'identifier les bénéficiaires effectifs et les liens entre l'origine et la destination des fonds en raison de l'utilisation de comptes intermédiaires ou de comptes de professionnels non financiers comme comptes de passage, ou du recours à des structures sociétaires complexes et à des montages juridiques et financiers rendant peu transparents les mécanismes de gestion et d'administration;

10° Les opérations financières internationales sans cause juridique ou économique apparente se limitant le plus souvent à de simples transits de fonds en provenance ou à destination de l'étranger notamment lorsqu'elles sont réalisées avec des Etats ou des territoires visés au 1°;

11° Le refus du client de produire des pièces justificatives quant à la provenance des fonds reçus ou quant aux motifs avancés des paiements, ou l'impossibilité de produire ces pièces;

12° Le transfert de fonds vers un pays étranger suivi de leur rapatriement sous la forme de prêts;

13° L'organisation de l'insolvabilité par la vente rapide d'actifs à des personnes physiques ou morales liées ou à des conditions qui traduisent un déséquilibre manifeste et injustifié des termes de la vente;

14° L'utilisation régulière par des personnes physiques domiciliées et ayant une activité en France de comptes détenus par des sociétés étrangères;

15° Le dépôt par un particulier de fonds sans rapport avec son activité ou sa situation patrimoniale connues;

16° La réalisation d'une transaction immobilière à un prix manifestement sous-évalué.

Appendix 3

Employee Suspicious Transaction Reporting Form to the AML Officer

Internal Suspicious Transaction Report to Your AML Officer

Your Name:	
Your MainFirst Entity/Business Unit:	
Date:	
Your Contact Details:	

Please complete as much of this form as possible for the company to which the suspicion relates:

Firm Name:	
Type of Business:	
Address:	
Indicate whether transaction performed/outstanding/rejected or NA:	
Further Details if needed (e.g. proxy, other participant details):	

Reason(s) for suspicion (please continue on a new page if necessary):

Signed:
Date:
On completion you should send a copy to Your AML Officer as soon as possible. **Important Note**: Employees are prohibited by law from disclosing ("tipping off") the fact that a suspicious transaction report or related information is being filed with the Financial Intelligence Unit (FIU) and the competent office of district attorney.

FOR AML OFFICER RECORDS ONLY:		**Reference No:**	
Date suspicion received:		**Date receipt provided for STR:**	
Reported to FIU: Y/N		**Date reported to FIU:**	
Response received from FIU: Y/N		**Date of response from FIU:**	
FIU reference details:		**Date of update to reporter & Management:**	
AML Officer suspicion report records updated: Y/N			

Appendix 4: Employee Internal Whistleblowing Reporting Form

Internal Whistleblowing Reporting Form to Compliance

Employee Name:	
Employee´s MainFirst Entity and Business Unit:	
Contact Details:	

The Internal Whistleblowing Process, as set out in the MainFirst Group Anti-Money Laundering, Counter-Terrorist Financing and Financial Crime Prevention (FCP) Policy, ensures that Employees who report information which, tend 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, may be reported anonymously to Compliance. Please read the Internal Whistleblowing Rules carefully prior to submitting this form. Complete as much of this form as possible for the activity to which the suspicion relates. Note that you do not need to have all the required information before contacting Compliance In urgent cases please contact Compliance quickly e.g. by telephone if appropriate, giving the basic details and reasons for suspicion. Any other information can be supplied subsequently:

Please describe the suspicious activity or situation[26] (to be filled out by Employee)
Have you discussed your concern with any person[27]**, your responsible Manager or did you escalate to the next Management level?**

[26] Please attach any documents to this reporting form that might be useful in order to clarify the incident.
[27] If you have discussed the incident with persons outside of MainFirst please provide full names and addresses.

(to be filled out by Employee)
Is there a reasonable suspicion of a criminal offence? If so, what is the reasoning? (to be filled by Compliance)

FOR COMPLIANCE RECORDS ONLY:	**Reference No:**
Date suspicion received:	
Internal Whistleblowing Rules applicable Y/N:	
Management/COO Information Y/N:	Date of Notice to Management/COO:
Further Action Taken Y/N:	Date of Notice to Employee:
Suspicious Activity Report submitted to relevant authority(-ies): Y/N	Date of submission:

Signature Compliance