Julius Bär

Document title:	JBG-2000-00 Group Financial Crime Policy
Effective date:	01/01/2020
Version:	1.0
Approved by:	Oliver Bartholet, Raimund Röhrich
Author:	Patrick Regamey
General scope:	Legal Entities worldwide

	Significant regulated entities	All other Advisory Offices	Group WMCs	Other
Julius Baer Group	Bahamas Germany Guernsey Hong Kong India Luxembourg Monaco (Bank) Singapore Switzerland (Bank) U.A.E. UK	Austria Bahrain Chile Ireland Israel Lebanon Monaco JBWM Russia South Africa Spain Uruguay	Fransad Gestion GPS Brazil JB Fiduciaria (Milano) JBWM Nomura Kairos NSC Wergen & Partner	

SUMMARY

The adoption of effective Financial Crime Compliance (FCC) standards is an essential part of Julius Baer Group's (the Group) risk management framework, detecting and preventing Financial Crime such as Money Laundering (ML), Sanctions and Embargos (SE), Terrorist Financing (TF), Bribery and Corruption (BC) and complying with all Financial Crime Risk related requirements and obligations set out in applicable legislations, regulations and industry guidelines. The Group actively manages and mitigates legal, regulatory and reputational Financial Crime risks globally through internal policies, procedures, systems and controls.

This policy outlines the Group FCC Policy Framework and defines the Governance principles to detect and prevent Financial Crime within the Group's activities and business relationships. These principles form the basis of the Group's commitment to standards as required by law and applied by the community of international private banks.

Key aspects of this policy

- Definition of the overall Group FCC Policy Framework
- Basic FCC principles concerning the detection and prevention of Financial Crime
- Duties and responsibilities of all employees related to FCC including escalation procedures
- Consolidated Supervision governance and processes for all FCC matters
- Definition of basic principles concerning trainings, records retention, confidentiality and contact with authorities in the area of Financial Crime

Violation of this policy may result in disciplinary action.

1. GROUP FCC POLICY FRAMEWORK

The Group FCC Policy Framework is composed of the below listed policies. This policy constitutes the umbrella policy of all Group policies related to FCC. Together, they set out the Group FCC Policy Framework as well as the related governance processes of the Group.

The Group FCC Policy Framework and related governance processes reflect the Group's commitment to ensure that the Group's services are not being misused for any type of illegal activity. The Group's robust FCC risk culture commitment is driven by the tone from the top, the risk awareness of the employees at all levels and clearly defined accountabilities.

1.1. Group FCC Policies

The Group FCC policies and accompanying standards are topic related and define principles, procedures and responsibilities of Financial Crime detection and prevention. In addition to this policy, the following Group FCC policies apply:

- JBG-2003-00 Private Banking Client Acceptance Policy
- D-1152-00 Client Acceptance and Maintenance Policy for Institutional Relationships
- JBG-2001-00 Global Anti-Money Laundering Monitoring Policy
- JBG-2002-00 Group KYC Standards
- JBG-2003-00 Identification & Verification
- D-1079-00 International Sanctions and Embargos
- D-1023-00 Gifts and Entertainment & Anti-Corruption Policy

The Group FCC policies are published, maintained and owned by the Group Financial Crime Compliance Unit (FCCU) at the head office in its global supervision function. The FCCU is responsible to inform local Compliance of any update or modification of the Group FCC policies in a timely manner to allow the other legal entities to implement the modifications. Transitional periods and measures might be defined, if required.

1.2. Exceptions and Deviations

Policies and procedures at Group entity level must be consistent with and supportive of the Group standards even where for local mandatory regulations such policies and procedures are not identical to the ones from the Group.

However, legal entities may have a need for exceptions to the Group FCC policies due to requirements of local regulations, business models or other local specific requirements. For exceptions relating to the implementation of the Group FCC policies in legal entities, the process defined in section "Request for exceptions to global policy (GMS) implementation" in the JBG-G-1004-00 Policy Management Framework Guideline needs to be followed. Exceptions are only granted if the legal entity

is able to demonstrate the need for the exception and if the local discrepancies are consistent with and supportive of the principles of the Group FCC policies.

Legal entities may also have the need for deviations to the Group FCC policies. A deviation occurs when the requirements of the Group FCC policies and accompanying standards are met, but local regulations, business models or other local specific requirements require a stricter standard to be applied. Legal entities of the Group are not required to seek approval for such deviations but must document them in a country specific policy.

2. BASIC PRINCIPLES

In the frame of the global supervision as required by Group's home regulator[1] and in line with international standards, the below FCC principles are applicable to all legal entities of the Group.

2.1. Risk Tolerance Framework

The Group CRO is responsible for maintaining and further developing the Risk Tolerance Framework (RTF) on behalf of the Executive Board of the Group and Executive Board of the Group's principal operating entity Bank Julius Baer & Co. Ltd. The Group Board of Directors (Group BoD) reviews and approves the content of the RTF at least annually. The RTF is describing how the risk tolerance and risk appetite of the Group is established, defined and implemented.

2.2. Risk Based Approach

The concept of a risk based approach is one of the key principles of sound risk management practices in the area of Financial Crime risks.

Following a risk based approach implies that the Financial Crime risks across the Group have to be identified and appropriate measures must be developed, which are commensurate with the actual nature and level of the risk identified. Thus, for increased risks, the corresponding measures have to be more rigorous and granular, while standard risks can be met with less rigorous measures.

2.3. Documentation

The Group shall prepare, organize and retain its documentation in such a way that qualified persons (e.g. authorities, auditors) can within reasonable time form an opinion whether the Group has complied with its responsibilities to detect and /or prevent Financial Crime.

Furthermore, the documentation shall be prepared, organised and maintained in such a manner that the Group is able to provide requested information to prosecuting authorities or other regulatory or enforcement authorities within a reasonable timeframe.

[1] Swiss Financial Market Supervisory Authority (FINMA).

2.4. Anti-Money Laundering / Combatting Terrorism Financing

As part of its efforts to prevent being used as a conduit for Financial Crime, the Group implements robust and consistent Anti-Money Laundering (AML) and Combatting Terrorism Financing (CTF) control measures.

2.4.1. Identification & Verification

The Group has to identify and verify the identity of the account holders and beneficial owners. Further, it has to check the identity of the persons that act on behalf of the client in establishing a relationship. For further details, reference is made to JBG-2003-00 Identification & Verification.

2.4.2. Know your Client (KYC)

KYC is the process of establishing comprehensive profiles of the Group's clients and verifying the content through reliable sources. KYC profiles must reflect the factual situation and circumstances of the clients in a comprehensive, up-to-date and accurate form. This entails the understanding of the client background, the Source of Wealth, Source of Income and Source of Funds, the intended purpose of the account, expected transactional behaviour and the potential existence of higher FCC risks, including adverse media or broader reputational risk. For further details, reference is made to JBG-2002-00 Group KYC Standards.

2.4.3. Transaction Monitoring

By taking into account its international franchise, its business model, its activities as well as complexity and the inherent ML and TF risks, the Group establishes its transaction monitoring systems to provide sufficient controls for the detection, investigation and reporting of unusual and/or suspicious transactions.

2.5. Sanctions and Embargoes

The Group is required to comply with applicable SE laws and regulations. SE may be imposed against countries as a whole, their nationals and/or residents of such countries or against individuals and entities in any country, irrespective of location. The Group screens new clients during the account opening process and the whole client base on a regular basis thereafter. Furthermore, the Group implements and maintains an electronic SE filtering system that monitors incoming and outgoing payments against SE lists. For further details, reference is made to D-1079-00 International Sanctions and Embargos.

2.6. Anti-Bribery and Corruption

The Group is committed to maintain the highest levels of ethical standards in relation to all its business activities and has zero tolerance for breaches of the applicable legislation related to BC. Its employees and legal entities must comply with international and local BC laws. Furthermore, the Group does not tolerate its employees being involved in acts of bribery and corruption. For further details, reference is made to D-1023-00 Gifts, Entertainment & Anti-Corruption Policy.

3. DUTIES AND RESPONSIBILITIES

3.1. Three Lines of Defence Model

As part of sound risk management principles, the Group has implemented the three lines of defence model.

The Front Office[2] as the first line of defence plays a critical role and shall be responsible for appropriately implementing internal controls and a control environment and culture anticipating misdemeanors related to the mitigation of Financial Crime risks and policy breaches.

As part of the second line of defence, Compliance monitors adherence to the Group FCC policies by carrying out regular checks and providing the oversight and tools, systems and advice necessary to support the first line of defence in identifying, managing and monitoring risks related to Financial Crime.

Group Internal Audit, as the third line of defence, is responsible for independently assessing processes and controls in the first and second line of defence, using a risk based approach.

3.2. Board of Directors

The Group BoD as the primary governing body is responsible for the approval of the overall risk management framework of the Group. The Group BoD reviews the Group's Financial Crime Risk Assessment (reference is made to section 5.1) and determines the Group's risk appetite. The Group BoD has the overall responsibility to ensure that the Group is equipped with the necessary resources to effectively manage and control its Financial Crime risks. Regarding the duties and responsibilities of the Group BoD in general, reference is made to D-1000-00 Organizational and Management Regulations of Julius Baer Group Ltd. and the Julius Baer Group.

3.3. Chief Executive Officer and Executive Board

The Chief Executive Officer and the Executive Board of the Group have the overall responsibility for organizational and operational measures. They initiate the necessary measures to comply with the relevant laws and regulations for the detection and prevention of Financial Crime. Regarding the duties and responsibilities of the Chief Executive Officer and the Executive Board of the Group in general, reference is made to D-1000-00 Organizational and Management Regulations of Julius Baer Group Ltd. and the Julius Baer Group.

[2] "Front Office" refers to relationship managers, assistant relationship managers, line managers of relationship managers, account managers, or other first line of defence employees.

3.4. Compliance Function

3.4.1. Group Financial Crime Compliance Unit

The FCCU constitutes the global FCC body of the Group and bears the main responsibility for all matters related to the prevention of Financial Crimes like ML, TF, SE as well as BC. It exercises the functional lead within the Group and is responsible for establishing adequate Group FCC policies, the implementation of and the adherence to the Group FCC policies by all Group legal entities in scope in order to ensure that Financial Crime risks are managed globally. The FCCU is the main point of contact for issues affecting the Group and/or international impact in connection with FCC related matters.

3.4.2. Local Compliance

Local Compliance is responsible for the local implementation and the adherence to the rules set out by the Group FCC policies. Where required, they are responsible for initiating the exception process (reference is made to section 1.2). Local Compliance is the first point of entry for any local issues with regard to FCC.

3.5. Employees

Employees at all levels, regardless whether they are first or second line of defence, are personally responsible for complying with the Group FCC policies within the scope of their activity including the local applicable FCC policies.

4. ESCALATION PROCEDURES

4.1. Escalation Procedure in case of Concerns or Suspicion

Employees must escalate to their superior and local Compliance immediately if they observe any business activity that raises concerns or the suspicion of a connection to Financial Crime. For further details, reference is made to JBG-2004-00 Group Investigations Policy and D-1286-00 JB Integrity Platform.

Local Compliance is responsible to review and assess the concerns or the suspicion escalated to them. For further details concerning the handling of a suspicion, reference is made to JBG-2001-00 Global Anti-Money Laundering Monitoring Policy .

The Group FCC policies define which cases have to be reported by local Compliance to Group Compliance such as the FCCU, Group PEP Desk or the Group Sanctions Desk. In addition, local Compliance is required to report certain events to Group Compliance (reference is made to section 5.2 below).

4.2. Escalation Procedure in case of Difference in Opinion between Front Office and Compliance

Where an agreement cannot be reached between Front Office and local Compliance with regard to a specific business case/relationship, the case shall be first escalated to the local Client Review Committee, if available, or to the Location Head and Local CRO. If required, the case may be escalated to the Region Head and Regional CRO, and further to Group CRO for final decision.

4.3. Policy Breaches

Any breach of the Group FCC policies poses a potential risk to the reputation of the Group and could result in legal action, including criminal prosecution or regulatory sanction.

The Group is committed to taking appropriate action against any misconduct related to Financial Crime. This includes reporting the matter to an appropriate government department, regulators, authorities or the law enforcement body and/or taking internal disciplinary action against relevant employees and/or terminating contracts with associated persons.

For this reason, employees have to immediately report any observed potential breach of the Group and/or local FCC policies to their superior and local Compliance. For further details, reference is made to JBG-2004-00 Group Investigations Policy and D-1286-00 JB Integrity Platform.

Non-compliance with any requirement of the Group and local FCC policies can lead to serious consequences for employees and/or their superiors, such as disciplinary measures as provided under employment law, up to and including summary dismissal. Failure to report observed misconduct by other employees may also results in disciplinary action.

5. CONSOLIDATED SUPERVISION

The Group shall identify, limit and supervise its legal and reputational risks related to Financial Crime on a global level. Therefore, the Group shall implement the following processes related to Financial Crime:

- Annual Financial Crime Risk Assessment (FCRA) process, both at local and Group level
- Ad-hoc reporting by the Group's legal entities of any local events leading to a significant change of the overall risk for the legal entity and /or Group
- Periodic risk based controls of the Group's legal entities including on-site controls by Group Compliance
- Subject to local restrictions and upon request, the legal entities of the Group make all relevant information available to the Group's organisational units responsible for the global monitoring of the legal and reputational risks
- Access to the information on individual relationships in all legal entities of the Group by Group Internal Audit and External Audit if the need arise.

5.1. Financial Crime Risk Assessment

The FCCU establishes an annual FCRA process in order to determine inherent risks, control effectiveness and the residual risks of the Group and related action plans.

The legal entities of the Group provide the FCCU with its annual local FCRA, which is a standardized assessment based on quantitative and qualitative data as defined by the FCCU. Based upon the local FCRAs, the FCCU establishes the Global FCRA

with the goal to assess the Financial Crime risks of the Group on a consolidated basis.

The results of the Global FCRA are reviewed and approved by the Executive Board of the Group and the Group BoD.

5.2. Ad-hoc Reporting

The Group's legal entities ensure a timely report to the Group about any local events leading to a significant change of the overall risk related to Financial Crime for the legal entity and /or the Group (ad-hoc reporting). The ad-hoc reporting is ensured for the following events:

- Account opening for and continuation of politically exposed person (PEP) relationships
- New relationships which have a significant impact[3] on the financial result of the legal entity
- Suspicious Activity Reports (SAR) or Suspicious Transaction Reports (STR) (thereafter collectively referred to as STR) filed by the Group's legal entities
- Any relationship or transaction connected to international ML and/or TF scandals, true matches for SE or serious BC misconduct by an employee, if not already covered by the STR Reporting
- Any other risk changes such as serious organisational deficiencies or serious failures of systems, which represent a significant change of the overall risk for the legal entity and /or the Group.

5.3. Periodic risk based controls by Group Compliance

The Group ensures periodic risk based controls of the Group's legal entities related to Financial Crime including on-site checks and controls by Group Compliance. The control framework covers the FCC design controls (e.g. assessment of the local FCC Framework and Governance, verification of compliance with the Group FCC Policy Framework) as well as the operational effectiveness of the FCC framework (e.g. sample checks of individual relationships). Scope and periodicity of the controls are defined based upon the findings of the FCRAs and other risk assessments, reporting, audit findings and the results of previous controls.

6. TRAINING

The Group FCC Policy Framework requires the Group to develop and maintain effective, on-going, risk based programmes aiming at training and educating all relevant employees related to Financial Crime risks. In particular, all new employees must be properly instructed/trained about their FCC duties in due time.

[3] A relationship has a significant impact on the financial result of a location if the expected assets under management represent 10% or more of the local Net New Money growth target.

Group Compliance is responsible for defining the scope, frequency and target groups of the relevant global training programmes. Furthermore, the FCCU provides guidance on the content, tools and format[4] of training and education programmes.

Local Compliance is responsible for the implementation of relevant training programmes locally and ensuring the timely accomplishment of it by all relevant employees. Where local law defines specific training requirements (e.g. for certain topics or employee categories), local Compliance includes such specific local requirements in their training programmes.

All training has to be tracked. The Group is required to maintain training records, e.g. name of employees trained, the date of the training, nature of training received and results of any training tests undertaken.

7. RECORDS RETENTION

All records created in connection with implementing and complying with the Group FCC policies, including, but not limited to customer records and all customer transaction records, must be retained in accordance to the D-1109-00 Global Archiving Policy for physical and electronic documents.

8. CONTACT WITH AUTHORITIES AND REGULATORS

The Group may receive requests from local authorities, law enforcement bodies or regulators in connection with FCC related questions and investigations. The Group is fully committed to cooperating with such requests within the confines of applicable laws and regulations.

Local Compliance acts as a contact point with the local authorities, law enforcement bodies and regulators and as recipient of all such regulatory requests. Any employee must direct any related contact requests by authorities, law enforcement bodies and regulators immediately to local Compliance, which ensures that these requests are managed properly and in a timely manner.

Any request by local and/or other authorities or regulators directly or indirectly affecting or being otherwise (potentially) of material relevance (including from a regulatory or reputation perspective) for the Group, or which have an international impact, must be escalated by local Compliance to the FCCU without delay. FCCU, local Compliance and the relevant organisational unit, will coordinate internal (management and other stakeholders) and external (regulatory authorities, external auditor etc.) reporting and respond to that request and act accordingly, whilst ensuring that responses are consistent with local privacy or other laws.

9. CONFIDENTIALITY

In managing its Financial Crime risks, the Group must ensure that all employees adhere to all applicable confidentiality requirements. These requirements include ensuring that all relevant employees are fully aware of the requirement not to disclose to any client or third party, either directly or indirectly, that they are subject to STRs,

[4] Training programme is delivered via the most appropriate format (e.g. web-based or as in-person/instructor-led training).

so as not to prejudice a review or investigation by law enforcement or a competent authority.

Client data is sensitive and shall not be filed in a generally accessible location. The access to this data is to be organised technically and organisationally in such a way that the information is only accessible by the relationship manager, his/her deputy, superior, Legal, Compliance, Internal Audit and Risk Management.

FS JBG-2000 Group Financial Crime Policy