Julius Bär

Document title:	JBG-2001-00 Global Anti-Money Laundering Monitoring Policy
Effective date:	01/01/2020
Version:	10.0
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

Julius Baer Group (the Group) implements robust and consistent Anti-Money Laundering (AML) and Combatting Terrorism Financing (CTF) on-going monitoring measures to ensure compliance with all applicable AML and CTF laws and regulations.

This policy outlines the principles regarding the Group's transaction monitoring as well as investigation and reporting of potential money laundering (ML) and/or terrorism financing (TF) suspicious activities and transactions. These principles form the basis of the Group's commitment to prevent being used as a conduit for financial crimes.

This policy adheres to the principles outlined in JBG-2000-00 Group Financial Crime Policy and is part of the Group's Financial Crime Compliance Framework.

Key aspects of this policy

- Key components of the Group's transaction monitoring framework: ongoing monitoring requirement, ex-ante (real time) payment screening and ex-post transaction monitoring
- General principles on performing transaction monitoring reviews
- Investigation and, where required, subsequent reporting of suspicious activities and transactions
- Follow-up measures after reporting of suspicious activities and transactions
- Information sharing within the Group and reporting to the Head Office

Violation of this policy may result in disciplinary action.

1. RESPONSIBILITIES

It is the responsibility of all employees of the Group to adhere to the requirements of this policy and to comply with applicable AML and CTF laws and regulations.

The implementation and maintenance of this policy is supported by the “Three Lines of Defence" model as part of the Group’s risk management framework.

The **first line of defence**, particularly the Relationship Manager (RM) and the superior of the RMs, represents the function that has ownership and management over the client risks in connection with the clients’ activities and transactions. The RM is responsible for understanding the clients’ transactions and retrieving relevant transaction background information. It is the duty of the RM to ensure that the client transactional behaviour corresponds to the client profile. In case of unusual and/or potentially suspicious activities or transactions, the RM is required to clarify with the client and/or to escalate to his/her superior and Compliance for further investigation, assessment and decision. Reference is made to sections 2.3 and 3.1 for further details. The superior is responsible for ensuring that the RM(s) under his/her supervision comply with this policy.

The **second line of defence**, particularly Compliance, is responsible for establishing the compliance-related risk management framework and the associated control standards. For transaction monitoring, Compliance independently reviews unusual and/or potentially suspicious activities or transactions and reports suspicious activities or transactions to the competent local authority – generally referring to the Financial Intelligence Unit of a country – by the locally designated Money Laundering Reporting Officer (MLRO) or his/her delegate.

The **third line of defence**, Internal Audit, provides independent analysis and risk assurance to the senior management on the effectiveness of the risk management framework and governance including ML and TF risks.

2. TRANSACTION MONITORING

2.1. Overview

Transaction monitoring is an essential component of the Group’s Financial Crime Framework and part of the Group’s effort to prevent its products and services being misused for the purpose of ML and TF. The objective of transaction monitoring is to identify, investigate and assess any unusual and/or potentially suspicious activities and transactions throughout the entire life cycle of client relationships and, if required, report to the competent local authority.

The Group adopts a risk-based approach to implement its AML and CTF framework and to enhance the effectiveness of transaction monitoring. Following a risk-based approach in the context of transaction monitoring, unusual and/or potentially suspicious transactions are distinguishable from legitimate transactions and the corresponding review is performed commensurate with the actual nature and level of ML and TF risks identified. The adoption of the risk-based approach enables the Group to manage its resources on combatting ML and TF risks in the most effective manner

and focus its efforts on transactions potentially posing a higher risk of ML and TF. By taking into account its international franchise, its business model, its activities and the inherent ML and TF risks, the Group establishes its transaction monitoring system to provide sufficient controls for the detection, investigation and reporting of unusual and/or potentially suspicious transactions involving higher risks.

In order to facilitate the transaction monitoring throughout the entire life cycle of client relationships, the Group has implemented the following ongoing monitoring framework:

- **Ongoing monitoring** – The RM is responsible for monitoring client accounts for any unusual and/or potentially suspicious activities or transactions[1]. The RM is required to "Know Your Client" (KYC) and "Know Your Transaction" (KYT). The RM shall remain vigilant for any unusual and/or potentially suspicious activities or transactions throughout the entire life cycle of client relationships. The existence of automated transaction monitoring systems does not supersede the requirement for on-going monitoring through RM's vigilance. Before executing the client's instructions, the RM shall be aware of the plausibility of the transactions and the consistency with the client profile. When circumstances demand to understand the background of the transactions and/or validate source of funds/wealth (i.e. not possible to plausibilise a transaction via open source, KYC etc.), the RM shall request transaction-related information and/or documentation from clients and duly maintain the client profile up-to-date in case of new KYC information. The RM shall escalate to his/her superior and Compliance for further assessment and decision whenever in doubt or in case of identification of unusual or potentially suspicious transactions through either client due diligence or automated transaction monitoring systems.
- **Ex-Ante (real time) payment screening** – The screening or filtering of payment messages prior to execution is to prevent the Group from making funds available to individuals, entities or countries in breach of the Group's policies or locally applicable sanctions and embargoes rules. For more details on real time payment screening, reference is made to policy D-1079-00 International Sanctions and Embargos.
- **Ex-Post transaction monitoring** – the Group adopts automated transaction monitoring systems to monitor transactions after the execution in order to identify unusual and/or potentially suspicious transactions, including unusual single transactions as well as transaction flow patterns. The automated transaction monitoring system adopts both threshold-based criteria and behaviour-based criteria to identify transactions with potentially elevated ML and TF risks

[1] "Unusual transactions" include but are not limited to:
(1) Transactions deviating from the expected or usual transactional behavior and/or the client profile;
(2) Transactions bearing indication of ML and TF listed in appendix JBG-2001-01 Indicators of Money Laundering and other ML red flags issued by local authorities.
For details on "suspicious activities and transactions", reference is made to footnote 4 below.

for subsequent review and, where required, report to the competent local authority by the MLRO or his/her delegate. With regard to the legal entities within the Group (i.e. advisory office) where the nature of the business and/or the volume of transactions do not warrant automated system solutions, manual transaction monitoring may be exceptionally applied in agreement with the Global Head of the Financial Crime Compliance Unit.

2.2. Prohibited Transactions

The Group and its employees are prohibited from facilitating the following types of transactions unless specified otherwise below:

- Transactions that are linked to informal fund transfer systems, also known as "Hawala Banking" or "Hundi"[2];
- Incoming transactions where the assets are known or suspected to be the proceeds of criminal activities, including predicated tax offences;
- Transactions where a non-client of a specific legal entity of the Group presents assets and submits instructions for delivery or forward to another non-client, or transactions for a client where no account is opened in any legal entity within the Group;
- Transactions which involve the settlement of client transactions through the Group's own accounts[3];
- Pass-through transactions where the incoming payment and the connected outgoing payment for the benefit of a third party are with no economic justification and the account holder is not the beneficial owner of the assets passed through the account. Third party pass-through transactions are only exceptionally accepted upon the Compliance approval under the following conditions:
  - Either originator or beneficiary of the transaction is the client of the Group and the transaction is booked on the respective account with the Group (external-external transactions are in general forbidden);
  - There is a plausible and legitimate purpose for such transactions and the purpose is not to hide the identity of the originator and the beneficiary;
  - The obligation of beneficial ownership identification and verification must be fulfilled;
  - The background and purpose of the transaction must be documented in a comprehensive manner.

[2] Hawala Banking is money transfer without money movement and simply based on "trust".
[3] "Group's own accounts" include the following internal accounts: suspense accounts, control accounts and transition accounts used for the sole purpose of reconciliation, P&L allocation and non-client related settlement.

2.3. Components of Transaction Monitoring Review

Transaction monitoring review is performed either on system-generated transaction alerts or on unusual and/or potentially suspicious transactions detected through other means (i.e. client due diligence). A transaction monitoring review is comprised of the following components. Through the application of these components by the reviewer (the RM, superior and/or Compliance), the Group ensures a consistent approach for transaction monitoring review. For more details on the handling of system-generated transaction alerts, reference is made to JBG-G-2001-00 Managing and Handling of Transaction Monitoring Alerts – Clarification Principles.

2.3.1. Purpose and Background of the Transactions

The reviewer shall understand the purpose and the economic or lawful background of the transactions. This is crucial in differentiating regular client transactional behaviour from unusual transactional behaviour. The level of scrutiny on each transaction monitoring review follows the risk-based approach and shall be commensurate with the level of inherent or perceived ML and TF risks associated with the transactions and the Group's knowledge of its clients. The better the Group knows its clients, the greater will be its ability to identify discrepancies between the detected transactions and the client profile and thus evaluate unusual behaviour.

All relevant transaction-related information has to be collected. The reviewer shall obtain information with regard to the originator of the incoming transaction as well as the beneficiary of the outgoing transaction. The relationship between the client and the counterparty (originator or beneficiary) has to be identified. The reviewer also needs to understand the purpose and nature of the transaction(s), and the origin of the assets. Where necessary, the transaction monitoring review can be extended to a wider context of the client's transaction history (including across multiple client accounts) and past system-generated alerts in order to get a holistic view of the client's transactional behaviour.

A plausibility check has to be performed on all collected information with regard to the purpose and the economic or lawful background of the transactions. This can be achieved by assessing the reasonableness of the information through comparing the transactions with the client's financial circumstances and with those of peer group clients of similar background. It shall be possible for any independent third party to comprehend and deduce the plausibility of the purpose and the background of the transactions.

2.3.2. Consistency with Clients' KYC profiles

Evaluation of the consistency between the transactional behaviour and the client profile is a key component of any transaction monitoring review. The flow of funds shall be assessed in a wider context of the client's profile and overall relationship with the Group. The KYC information collected during client on-boarding and throughout the entire life cycle of client relationships facilitates the reviewer to form a holistic view of the client and the Group's risk exposure posed by the client.

The reviewer shall evaluate whether the detected unusual transaction(s) match the overall picture of the client relationship and are in line with the purpose and expected behaviour of the client relationship. Unusual transactions may not be suspicious if the KYC information or the client's business background provides sufficient grounds to consider the detected transactions as plausible and/or in line with the purpose and expected transactional behaviour of the client relationship. On the other hand, a material discrepancy or inconsistency raises a red flag and must be further assessed. Additional information, supporting documentation or clarification from the client shall also be requested where necessary. In case of new KYC information obtained during the transaction monitoring review, the RM shall duly maintain the client profile up-to-date.

2.3.3. Validation and Corroboration

In order to verify the details of the underlying transactions, the transaction monitoring review on the detected unusual transactions requires validation and/or corroboration, where necessary.

One of the main sources for the validation and corroboration is the information and/or supporting documentation received from clients. Transaction background information and/or supporting documentation shall be requested from the client whenever such information cannot be derived from the original client instruction, the payment remittance information or any KYC information on file. Media screening on the parties involved in the transaction (i.e. the client, the counterparty) and the related businesses is another source of information and may facilitate the review on unusual transaction(s). It supports the plausibility check on the transaction clarification provided by the client or reveals any potential indication of ML and TF risks associated with the parties or transaction(s). Information and supporting documentation from reliable external third parties may also be requested where necessary.

Corroboration refers to obtaining reliable information and/or supporting documentation where necessary, which supports the verification of the information provided by the client. Following a risk-based approach, the level of corroboration required depends on the available transaction-related information and various risk factors, and in general, the higher the risk of the client and/or the transaction(s) the more robust the corroboration needs to be.

2.3.4. Documentation

The reviewer must maintain sufficient documentation in the transaction monitoring system or in the appropriate archive system where required by the local policies or guidelines so as to evidence the investigation and assessment on the detected unusual transaction(s). The transaction monitoring review must be documented in such a way that any independent third party (i.e. senior management, auditor, regulator etc.) is able to understand the transaction background and the reasoning leading to the conclusion.

3. INVESTIGATION AND REPORTING OF SUSPICIOUS ACTIVITIES OR TRANSACTIONS

3.1. Investigation

All employees of the Group are required to escalate to his/her superior and Compliance any potentially suspicious activities or transactions[4], which may be associated with ML and TF risks during client on-boarding and throughout the entire life cycle of client relationships at the earliest possible time for further investigation and decision. Compliance will conduct a thorough investigation and assessment on the suspicious activities or transactions where appropriate and determine whether it is necessary to report to the competent local authority or take other appropriate measures. The investigation must be conducted in a timely manner as required by the applicable local laws and regulations.

3.2. Reporting

3.2.1. Suspicious Transaction Report (STR)

A Suspicious Activity Report (SAR) or Suspicious Transaction Report (STR) (thereafter collectively referred to as "STR"[5]) is filed with the competent local authority where there is suspicion of ML and TF related to prospects[6] or existing clients in adherence with the local laws and regulations. The locally designated MLRO[7] or his/her delegate ultimately decides on whether it is necessary to file a STR based on the Compliance assessment. The MLRO (his/her delegate) or the designated Compliance team is responsible for the filing of a STR with the competent local authority without any undue delay, i.e. within the timeframe as required by the applicable local laws and regulations.

The STR must contain sufficient information, which describes the trigger(s) to prompt the report filing, the assessment of the suspicion in the activities or transactions, and the nature of the (predicate) offence of ML and/or TF. Compliance maintains sufficient documentation on file in accordance with the relevant Group policies and the

---

[4] "Suspicious activities and transactions" include but are not limited to:

(1) Transactions bearing indication of ML and TF listed in appendix JBG-2001-01 Indicators of Money Laundering and other ML red flags issued by local authorities without sufficient and plausible explanation;
(2) Financial crime-related adverse information on the client or any counterparty identified through media screening or third-party communication;
(3) The unusual activities or transactions deviating from the client profile without sufficient and plausible explanation;
(4) The client's reluctance of providing any information or corroboration for the source of wealth/funds and/or the deviation from the expected or usual transactional behavior or the overall client profile.

[5] When referring to the reporting of suspicious activities or transactions, different jurisdictions use different terms - SAR, STR or both, and sometimes in different contexts. For the purpose of this Policy, these terms are collectively referred to as "STR".

[6] The term "prospect" refers to a potential client who has not entered into a formal business relationship with the Group.

[7] The MLRO must be a member of Compliance at the management level who oversees the legal entity's AML and CTF framework, and typically, is the Head Compliance of a legal entity or equivalent (i.e. the local Chief Risk Officer with a dual function as the local Head Compliance).

applicable local record-keeping laws and regulations, including all STRs filed together with supporting documentation as well as Compliance assessments for all STRs.

3.2.2. Prohibition of Tipping-off

All employees of the Group are explicitly prohibited from directly or indirectly disclosing any STR-related information to a client or third parties. Any unauthorised disclosure (also known as "tipping-off") is a violation of the reporting confidentiality requirement and may constitute a criminal offence in some jurisdictions. The Group ensures that during the course of filing STRs utmost care is undertaken to guarantee such reports are treated with the required level of confidentiality.

3.2.3. Post-STR Follow-up

Where required by the applicable laws and regulations, the MLRO (his/her delegate) or the designated Compliance team shall liaise with the competent local authority with regard to guidance on the execution of transactions or the handling the reported client relationship(s), i.e. whether and when termination of client relationship(s) and/or deposits/withdrawals of assets are permitted. The competent local authority may notify the legal entity whether it can continue to operate the account(s) as normal. Upon filing a STR, the account(s) may be subject to blocking measures as required by the local laws and regulations or from a risk control perspective. For the blocked accounts, transactions will be subject to the Compliance approval.

At the time of the STR filing or as permissible by the locally applicable laws and regulations, Compliance performs an appropriate appraisal of the client relationship in accordance with the Group's Risk Tolerance Framework. Based on the outcome of the appraisal, Compliance issues a recommendation to the responsible RM on whether the client relationship can be maintained (accepted or retained) or not. Where the Front Office[8] does not agree with the recommendation by Compliance regarding the acceptance or retention of a client relationship, the case must be escalated as per the escalation procedure defined in JBG-2000-00 Group Financial Crime Policy.

In case of a decision to exit the client relationship after a STR filing, refer to the details in JBG-2003-00 Private Banking Client Acceptance Policy and D-1152-00 Client Acceptance and Maintenance Policy for Institutional Relationships. In case of a decision to accept or retain the client relationship after a STR filing, the decision shall be approved by local Senior Management and appropriate enhanced measures are to be taken to manage the elevated ML and/or TF risks associated with the client relationship. The measures include but are not limited to heightened scrutiny of the account(s), increase of the client risk rating and/or restriction on the expansion of the client relationship. The RM must immediately escalate to his/her superior and Compliance whenever any further ML and/or TF risk indication becomes apparent. Compliance then decides if another or a follow-up STR is warranted.

[8] "Front Office" refers to RMs, assistant RMs, superiors of RMs, account managers, or other first line of defence employees.

All appraisals and decisions on the client relationships after the STR filing must be documented and stored by Compliance in the appropriate archive system.

3.2.4. Non-reporting

Certain unusual or potentially suspicious activities or transactions in question may not result in the filing of a STR due to lack of specific evidence justifying suspicion of ML and TF risks. In such circumstances, Compliance may determine additional scrutiny for on-going monitoring, appropriate measures (including conditions) or termination of the client relationship as deemed appropriate and necessary.

In case of non-reporting decisions due to insufficient suspicion, the rationale for not filing the STR and, where applicable, the risk mitigation measures need to be documented by Compliance in the appropriate archive system.

3.2.5. Information Sharing within the Group and Reporting to Head Office

A legal entity within the Group may share the information of a STR filing with the Head Office or other legal entities within the Group as permissible by the locally applicable laws and regulations. The legal entities involved in a cross unit relationship (CUR) shall inform each other before the STR filing or, if not permissible by the locally applicable laws and regulations, immediately after the STR filing. For further details, reference is made to D-1095-00 Cross Unit Relationship (CUR).

As part of the Group's consolidated supervision and oversight requirement, local Compliance is mandated to report to the Financial Intelligence Unit at the Head Office on an ad-hoc basis the following:

- any STR filing, either before the filing or, if not permissible by the locally applicable laws and regulations, immediately after the filing;
- any client relationship(s) or transaction(s) connected to internationally-known ML/TF scandals if not already covered by the STR filing.

In addition, local Compliance is also required to compile a monthly report regarding all STR filings in order for the Financial Intelligence Unit at the Head Office to identify and assess ML and TF threats as well as risk-related trends and patterns on a group-wide level.

Appendix:

– Appendix 1: JBG-2001-01 Indicators of Money Laundering

FS JBG-2001 Global Anti-Money Laundering Monitoring Policy