VIA BRASIL

AML POLICY, COMBATING THE FINANCING OF TERRORISM AND COMBATING THE FINANCING OF THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION

1. EXECUTIVE SUMMARY

1.1 The Policy for Preventing and Combating Money Laundering, Terrorist Financing and Proliferation of Weapons of Mass Destruction ("Policy") establishes the principles, guidelines and describes VIA BRASIL's internal controls to prevent and combat money laundering, terrorist financing and proliferation of weapons of mass destruction ("Policy"), in accordance with the legislation and regulations in force (in particular Law No. 9,613/1998, Law No. 13,260/2016, the applicable sanctions legislation and the resolutions of the COAF/Financial Intelligence Unit – UIF) and with good practices in the national and international market, for the identification of operations and/or situations that present atypicality that may constitute evidence of Money Laundering and/or Terrorist Financing and/or the Financing of the Proliferation of Weapons of Mass Destruction.

2. OBJECTIVE

2.1. The main objectives of this Policy are: 1) to conduct its business by VIA BRASIL in accordance with the highest ethical standards and to avoid establishing any commercial relationships or transactions that may contradict the principles and guidelines defined herein; including relationships with persons, entities or countries subject to national or international sanctions; 2) to establish the procedures for checking the integrity of the individuals and legal entities with which VIA BRASIL relates or intends to relate; 3) to prevent VIA BRASIL from being held liable for acts of third parties contrary to the provisions of this Policy; and, 4) assist and cooperate with law enforcement authorities to prevent money laundering and the financing of terrorism and/or weapons of mass destruction.

2.2 VIA BRASIL will take the necessary measures against any form of transformation of resources originating from illegal activities into assets of apparently legal origin, through the programming of training and the use of technological tools, in order to avoid transactions or situations that may be, directly or indirectly, linked to the crimes typified in Law 9.613/98, as well as the crimes of financing terrorism (Law No. 13,260/2016) and financing the proliferation of weapons of mass destruction, including when related to nuclear, chemical, biological or radiological weapons programs.

2.3. COAF stands for Financial Activities Control Council. COAF is an administrative entity linked to the Central Bank of Brazil and acts both as a control and intelligence authority and as a regulatory agency. The scope of COAF includes regulating, analyzing, and identifying illegal activities listed in Law No. 9,613/1998 and deciding and imposing administrative sanctions as necessary to the extent of its jurisdiction. COAF also performs the function of Financial Intelligence Unit (FIU), receiving, analyzing, and disseminating to the competent authorities communications of suspicious and automatic transactions.

4. REGULATORY ENVIRONMENT

I. Federal Law No. 9,613 of 03/03/1998 and subsequent amendments;

II. Federal Law 13,260 of 03/16/2016;

III. Federal Law No. 12,846 of 08/01/2013 regulated by Decree No. 11,129/22;

IV. Federal Law No. 13,709 of 08/14/2018;

V. Resolution No. 23/2012 – of the COAF (UIF);

VI. Resolution No. 29/2017 – of the COAF (UIF); e

www.viabrasil1.com
contato@viabrasil1.com
+55 11 99999-0934
Av. Paulista, 1636 - Conj 4 - Pavimento 15
Bela Vista, São Paulo - SP

VII. Normative Instruction No. 1571 - 07/02/2015 of the (RFB);

VIII. Resolutions of the COAF/UIF that provide for policies, procedures and internal controls of PLD/FT/FP (including subsequent rules that may replace or complement those mentioned);

IX. Brazilian normative acts that implement the resolutions of the United Nations Security Council (UNSC) on terrorism, its financing and financing of the proliferation of weapons of mass destruction.

5. RISK AND COMPLIANCE AREA

5.1. To communicate to COAF (UIF) the operations or situations suspected of involvement with the crimes provided for in Law 9,613/98 and Law No. 13,260/2016, as well as with the financing of the proliferation of weapons of mass destruction, within the maximum period provided for in the applicable regulations, counted from the internal decision to classify the operation as suspicious, upon resolution of the Board of Directors;

5.2. Properly store in physical and/or electronic media all documentation related to the activities related to this Policy for a minimum period of five years (or for a longer period, if required by specific rule or by determination of a competent authority).

6. COLLABORATORS

6.1. Report to the Risk and Compliance Area any and all operations, proposed operations or atypical situations, as well as those that, due to their form, value or habituality, constitute an artifice that aims to circumvent VIA BRASIL's identification, controls and registration mechanisms; including, but not limited to, payments or receipts by third parties without proven economic justification, commercial triangulations without business logic, operations with financial institutions in high-risk countries, operations incompatible with the declared economic and financial capacity, or any signs of sanctions violations.

7. GOVERNANCE

6.1.1. VIA BRASIL has a Risk and Compliance area that reports to the Executive Board. This team oversees the Policy and is responsible for a series of activities, such as regulatory mapping, maintenance of policies and risk measurement mechanisms, working with programs (KYC – Know Your Client, KYB – Know Your Business, KYS – Know Your Supplier, KYE – Know Your Employee, SAM-Suspicious Activity Monitoring, SAN- Sanctions Screening) and shared services, when applicable (Internal Audit), as well as establishing periodic meetings with the Board of Directors, and advising new product initiatives to define

www.viabrasil1.com
contato@viabrasil1.com
+55 11 99999-0934
Av. Paulista, 1636 - Conj 4 - Pavimento 15
Bela Vista, São Paulo - SP

Compliance requirements and appropriate controls to facilitate the launch of these with business teams. In addition to the dedicated Risk and Compliance team, the Executive Board is also committed to the effectiveness and adequacy of this Policy and its internal procedures and controls.

8. KNOW YOUR CLIENT (KYC) PROGRAM

8.1. Any client that trades in the precious metals market, especially gold MERCHANDISE, or FINANCIAL ASSET, which is a common legal entity, jewelry company, mining company, financial institution and foreign client will be considered as Clients. Clients who are financial institutions, intermediaries or international traders, as well as clients based in high-risk or low-transparency jurisdictions, will be subject to enhanced due diligence, in line with the risk-based approach of this Policy.

8.2. In the case of a legal entity, it is essential to know who the owner of the company is and what the shareholding composition is until reaching the natural persons authorized to represent it, as well as the chain of equity participation until reaching the natural person characterized as the final beneficiary, that is, the one who exercises control or significant influence in the management. VIA BRASIL will not maintain a relationship with clients whose corporate structure prevents the identification of the final beneficiary in an adequate and documented manner, except for exceptions provided for by law (for example, widely dispersed publicly-held companies), duly justified and approved by the Risk and Compliance Area.

8.3. Clients considered to be at high risk may be subject to an Enhanced Due Diligence (additional verification stage) throughout the life cycle of their relationship with VIA BRASIL, including appropriate measures to understand the corporate and control structures of legal entity sellers, to identify their final beneficiary. Any warning signs may result in requests for information, actions on the accounts or reporting to COAF. The enhanced due diligence should include, when applicable, analysis of restrictive lists and sanctions, negative media research, validation of the origin of funds and compatibility between the volume of operations, revenues and the client's economic and financial capacity.

8.4. In the case of Customers residing abroad, the company must adopt at least two of the following measures: 1-request an express statement from the customer regarding its qualification; 2- To resort to available public information; and 3- consult public or private databases on politically exposed persons. In addition, the country of incorporation, the country of main operation, the existence of applicable international sanctions, as well as the risk of the jurisdiction being classified as high risk or non-cooperative by international bodies (e.g., FATF) should be assessed.

9. KYC CHECKING

9.1. The restrictive lists must be checked at the Client's entry and in the respective registration updates. If it is found that the Client is on any impeding list or has been cited in any illegal event reported by the media, the Risk and Compliance Area must be notified to assess the beginning or maintenance of the relationship. The required registration documentation must be stored in electronic or physical media, including evidence of consultations and research carried out during the registration process. VIA BRASIL will specifically evaluate situations of "relevant negative media" (negative news) related to financial crimes, environmental crimes, human rights violations, corruption, sanctions and previous crimes of money laundering, and may refuse or terminate relationships considered incompatible with this Policy.

9.2. It is mandatory to check the following sources: Financial Activities Control Council COAF (UIF): List of politically exposed persons - SISCOAF; Office of Foreign Assets Control (OFAC): U.S. Anti-Terrorism List; and Other documents and information at the discretion of VIA BRASIL.

9.3. It is forbidden to establish or maintain a relationship with customers, suppliers or other partners that are sanctioned parties, or that act on behalf of or under the control of sanctioned parties, when such relationship may violate national or international sanctions applicable to VIA BRASIL.

KNOW YOUR SUPPLIER (KYS)

9.4. Based on good market practices, VIA BRASIL requires all its employees to properly identify the new Partner prior to the beginning of the relationship and execution of a formalized contract and where compliance with this Policy and good business practices will be mentioned. Suppliers considered to be at high risk – including mining companies in sensitive regions (border, conflict areas or high-risk according to the OECD/CAHRA), with a history of relevant environmental fines, evidence of the use of irregular labor or involvement in illegal mining – will be subject to enhanced due diligence and specific approval from the Risk and Compliance Area and the Board.

9.5. VIA BRASIL will not accept as a supplier: individuals or legal entities potentially involved with negative images and possible criminal practices; and Companies whose documentation and/or conduct does not allow the legitimacy of their activities to be identified; and existence of facts, which, at the discretion of VIA BRASIL, discredit the company and its owners. Suppliers that are on relevant national or international sanctions lists will also not be accepted, as well as those for whom it is not possible to reasonably prove the lawful origin of the gold or other precious metals supplied.

KNOWING THE TRACEABILITY OF THE GOLD SUPPLY CHAIN

9.6. The compatibility between the company's activity, its assets, its presumed financial capacity, as well as the origin of the resources used and the traceability of the mineral origin must be verified, by means of a certificate of procedural regularity issued by the National Mining Agency and environmental licensing, issued by the respective competent environmental authority. Whenever applicable, documents must be obtained that demonstrate the lawful origin of the ore and compliance with environmental and labor legislation, prohibiting the hiring of suppliers linked to illegal mining, protected areas, indigenous lands, conservation units or work situations in conditions analogous to slavery.

9.7. Among the measures adopted for the traceability of the gold supply chain, VIA BRASIL has the PRECIOUS METALS ORIGIN VERIFICATION POLICY, to ensure that the metals traded have a lawful origin, as well as are in compliance with Brazilian legislation, considering environmental and human rights aspects. This Policy shall be applied in an integrated manner with this PLD/FT/FP Policy, with a special focus on high-risk suppliers, operations with volumes incompatible with the declared production capacity and transactions involving jurisdictions classified as conflict or high-risk areas by the OECD (CAHRA).

10. SURVEILLANCE

10.1. Operations or situations that deviate from the expected standard must be communicated to the Compliance department for proper treatment. This action is essential to support the reporting to COAF (UIF). Discrediting news and, especially, related to financial crimes must be continuously monitored in order to mitigate image risk. The monitoring should consider, among other aspects, operations incompatible with the economic profile of the customer or supplier, commercial triangulations without economic justification, payments or receipts made by or for third parties without a legitimate relationship, recurrent use of transit accounts, operations with financial institutions located in tax havens or high-risk countries, as well as any sign of possible evasion of sanctions.

RISK-BASED APPROACH

10.2. The factors, drivers or risk drivers must be observed according to the conditions or characteristics that make a customer susceptible to being used to launder money, so compliance analyses will take into account the customer's commercial segment and tradition; nature of the activity and how much has been on the market; Geographic location of the client (risk jurisdictions and border regions); PEP; and source of funds (billing and equity).

The degree of exposure to sanctions, the use of complex corporate structures, the existence of relevant negative media history, and involvement with higher-risk gold and precious metals supply chains will also be considered.

10.3. Clients active in the Company will be classified by degree of risk:

LOW RISK: Corporate Customers – (Banking Institution and Metal Refiners).

MEDIUM RISK: Corporate Clients – (Jewelry, Mining Companies and Foreign Clients with more than 12 months of activity).

HIGH RISK: CORPORATE CUSTOMERS – (Jewelry, Mining Companies and Foreign Customers with less than 12 months of activity).

The above classification may be revised by the Risk and Compliance Area, if other relevant risk factors (e.g., country of incorporation, exposure to sanctions, negative media, volume of transactions, payment method) justify the reclassification of the client.

10.4. Customers classified as HIGH RISK must prove bank reference and bank qualification. Extra documents and information (e.g., financial statements, commercial contracts, proof of origin of funds and audit reports) may also be required, at the discretion of the Risk and Compliance Area.

11. PEP MONITORING PROGRAM AND RESTRICTIVE LISTS

11.1. To avoid the violation of targeted financial sanctions and to monitor its customers, VIA BRASIL will apply preventive, detection and risk-based reporting controls to the services it offers. These controls will include preventing the entry of addresses from restricted countries, screening customer name and address information, investigating and acting on suspicious mailing lists, denied party lists or possible links to sanctioned countries, and reporting (where necessary).

11.2. VIA BRASIL will also apply preventive and detection screening to politically exposed persons ("PEP"). This screening process will be done at the time of registration, periodically and in case of change of circumstances. If there is a match on the PEP lists, the case will be forwarded to the appropriate team for further analysis (Enhanced Due Diligence) and will be subject to the approval of the Risk and Compliance Area. Operations with PEP, their family members and close collaborators will always be treated as high risk, subject to reinforced monitoring, analysis of compatibility between equity, presumed income and volume transacted, which may result in refusal, restriction or termination of the relationship, according to risk assessment.

12. SUSPICIOUS ACTIVITY MONITORING PROGRAM (SAM)

12.1. The Suspicious Activity Monitoring Program reduces reputational and regulatory risk through the detection and management of related alerts, as well as reporting of suspicious activities, with possible indication of money laundering, terrorist financing and weapons of mass destruction or other illicit activities. This program will cover specific rules for monitoring transactions and customers and will consider regulated populations and risk behaviors identified in the Brazilian market, according to product vulnerabilities and possible modus operandi. Among the scenarios to be observed, the following stand out, without prejudice to others: (i) payments or receipts by third parties without economic justification; (ii) commercial and financial triangulations with multiple actors without business logic; (iii) repeated use of accounts in financial institutions in high-risk countries; (iv) fractional operations to avoid carry-over limits; (v) operations incompatible with the declared economic and financial capacity; (vi) discrepancies between the origin of the declared gold and the production capacity or documentation presented by the suppliers.

REGULATORY REPORTING AND THE RULE OF CONFIDENTIALITY (TIPPING-OFF)

12.2. VIA BRASIL's employees are prohibited from violating the confidentiality of investigations and reports to COAF, which is why they should not, under any circumstances, disclose the fact that a client is being investigated and that a report will be/has been forwarded to COAF, or any other information that may prejudice any related investigation. Information about the case should only be communicated to COAF and the competent legal authorities, as well as only to VIA BRASIL employees who have a real need. It is expressly forbidden to practice the so-called "tipping-off", that is, to warn, suggest, insinuate or allow the customer, supplier, partner or any third party to become aware of internal analysis, investigation or communication of suspicious transactions, under penalty of disciplinary and regulatory liability.

13. PAYMENTS AND RECEIPTS

13.1. PURCHASE TRANSACTIONS

13.1.1. Purchase transactions (gold, or other precious metals) must be paid by VIA BRASIL by means of Available Electronic Transfer (TED) or any other bank transfer order, including international SWIFT, issued to the seller and that the funds are credited to the deposit account held by the seller; Payment in cash, bearer checks or through third-party accounts without a legitimate and proven contractual link with the operation is prohibited. When intermediary financial institutions participate, their suitability and domicile jurisdiction must be evaluated from the perspective of PLD/FT/FP risk and sanctions.

13.2. SALES TRANSACTIONS

13.2.1. Sales and export operations may be received by VIA BRASIL by means of Available Electronic Transfer (TED) or any other bank transfer order of funds, including international SWIFT, international remittances, issued by the buyer and that the funds are debited from the deposit account held by the buyer. Payments made by unidentified third parties or without a direct and proven commercial relationship with the buyer will not be accepted, as well as payments in cash or through financial institutions located in high-risk jurisdictions or subject to sanctions, except after analysis and express authorization by the Risk and Compliance Area and the Executive Board.

13.3. THIRD-PARTY PAYMENTS AND TRIANGULATIONS

13.3.1. Payments or receipts on behalf of third parties, as well as commercial and financial triangulations involving more than two parties, will only be admitted when there is clear economic justification, adequate supporting documentation and prior approval from the Risk and Compliance Area.

13.3.2. Situations in which the origin or final destination of the funds are not clearly identifiable, or in which third parties are used only to interpose layers in the transaction, shall be treated as high risk and evaluated for possible communication with COAF.

14. TRAINING

14.1. Training is mandatory for "all" VIA BRASIL employees, as well as everyone who is directly involved in the operation. Administrators, agents, commercial representatives, outsourced employees who work in sensitive activities, as well as partners with management powers will be included, whenever applicable.

14.2 All training must contain the theme that deals with "PREVENTION OF MONEY LAUNDERING AND FINANCING OF TERRORISM AND WEAPONS OF MASS DESTRUCTION", and its renewal is mandatory within a period not exceeding 24 months. The contents will include, at least: concepts of money laundering, terrorist financing and proliferation; risk-based approach; KYC/KYB/KYS/KYE; final beneficiary; PEP; national and international sanctions; use of lists; identification of suspicious operations and situations; sealing to tipping-off; reporting procedures to COAF; and particularities of the gold and precious metals sector.

15. KEEPING AND MAINTAINING RECORDS AND DOCUMENTS, AND RECORDING TRANSACTIONS

15.1. VIA BRASIL will ensure that the custody and preservation of customer records and documents is implemented for an individual five (5) years after the closure of the account, unless an exception is defined. The records must allow the reconstruction of any relevant operation, including data of parties involved, amounts, dates, payment method, bank accounts used, intermediary financial institutions, supporting documents and, where applicable, evidence relating to the origin of the gold and the supply chain. In cases of ongoing investigation, notification of authority or litigation, the records must be kept until the definitive conclusion of the case, even if for a period of more than five years.

16. REPORTING SUSPICIOUS TRANSACTIONS

16.1. If VIA BRASIL suspects that the funds are proceeds of criminal activity or are related to the financing of terrorism, the transaction or proposed transaction will be promptly communicated to the Financial Activities Control Council (UIF) within a period not exceeding that established in the current regulations, counted from the moment the transaction is internally classified as suspicious, within 45 days after the decision to acknowledge the occurrence. The eventual decision not to conclude the operation does not remove the duty to communicate to COAF, when there is sufficient evidence of suspicion.

16.2 If VIA BRASIL suspects that the origin of the metal is different from that declared by the customer, or that the volume transacted is higher than that considered feasible by VIA BRASIL, the company will communicate to COAF (UIF) in the same terms. Situations involving possible illegal gold mining, protected areas, indigenous lands, use of labor in degrading conditions or any serious violations of environmental and human rights legislation will also be evaluated for the purpose of communication to COAF, in line with sectoral regulations.

16.3. VIA BRASIL refrains from providing its customers or third parties with information on any communications made as a result of evidence of money laundering or terrorist financing or weapons of mass destruction. Violation of this rule constitutes serious misconduct, subject to internal disciplinary measures and possible administrative sanctions by COAF and other competent authorities.

16.4. VIA BRASIL will deliberate on communications to COAF (UIF) in accordance with Resolution No. 23 of 12/20/2012. The body responsible for the deliberation (Executive Board, Committee or equivalent) must keep a formal record of decisions, including those in which it is concluded that there is no communication, with due justification, for the purposes of traceability and accountability to the authorities.

VIA BRASIL

ANNEXES – ALERT SITUATIONS

I SITUATIONS DERIVED FROM THE CUSTOMER IDENTIFICATION PROCESS:

i. Resistance to providing information necessary for the beginning of a relationship or for updating the registration;
ii. Offering false information;
iii. Provision of information that is difficult or costly to verify;
iv. Opening, handling of accounts or carrying out operations by a holder of power of attorney or any other type of mandate;
v. Occurrence of irregularities related to the procedures for identification and registration of operations required by current regulations;
vi. Registration of several accounts on the same date, or in a short period, with deposits of identical or approximate amounts, or with other elements in common, such as origin of funds, holders, attorneys-in-fact, partners, address, telephone number, etc.;
vii. Operations in which it is not possible to identify the final beneficiary, observing the procedures defined in the current regulations;
viii. Representation of different legal entities or organizations by the same attorneys or legal representatives, without reasonable justification for such occurrence;
ix. Information of the same residential or commercial address by natural persons, without demonstration of the existence of a family or commercial relationship;
x. ncompatibility of the economic activity or billing reported with the standard presented by customers with the same profile. including buying and selling volumes of gold and precious metals disconnected from the stated operational capacity, the physical structure observed in visits and the client's market history
xi. Registration of the same e-mail or internet protocol (IP) address by different legal entities or organizations, without reasonable justification for such occurrence;
xii. Registration of the same e-mail address or internet protocol (IP) by natural persons, without reasonable justification for such occurrence;
xiii. Information and documents submitted by the client that conflict with the publicly available information;
xiv. Partners of companies without apparent financial capacity for the size of the declared business activity.

II – SITUATIONS DERIVED FROM SITUATIONS RELATED TO PERSONS OR ENTITIES SUSPECTED OF INVOLVEMENT IN TERRORIST FINANCING AND THE PROLIFERATION OF WEAPONS OF MASS DESTRUCTION:

I. Financial transactions involving persons or entities related to terrorist activities listed by the United Nations Security Council (UNSC);

II. Operations or provision of services, of any value, to persons or entities that are known to have committed or attempted to commit terrorist acts, or participated in or facilitated the commission thereof; the existence of resources owned or controlled, directly or indirectly, by persons or entities known to have committed or attempted to commit terrorist acts, or participated in or facilitated the commission thereof;

III. Movements with indications of terrorist financing; financial transactions involving persons or entities related to the proliferation of weapons of mass destruction listed by the UNSC;

IV. Operations or provision of services, of any value, to persons or entities that have known to have committed or attempted to commit crimes of proliferation of weapons of mass destruction, or participated in or facilitated the commission thereof;

V. Existence of resources owned or controlled, directly or indirectly, by persons or entities that have known to have committed or attempted to commit crimes of proliferation of weapons of mass destruction, or participated in or facilitated the commission thereof;

VI. Movements with indications of financing the proliferation of weapons of mass destruction.

III – SITUATIONS RELATED TO EMPLOYEES, PARTNERS AND THIRD-PARTY SERVICE PROVIDERS:

i. Unusual change in the living standards and behavior of the employee, partner or outsourced service provider, without apparent cause;

ii. Unusual modification of the operating result of the partner's legal entity, including correspondent in the country, without apparent cause;

iii. Any business carried out in a manner other than the formal procedure of the company by an employee, partner, including correspondent in the country, or third-party service provider;

iv. Provision of assistance or information, paid or unpaid, to a client to the detriment of the company's anti-money laundering and terrorist financing program, or assistance in structuring or fractioning operations, circumventing regulatory or operational limits.

IV- SITUATIONS RELATED TO OPERATIONS CARRIED OUT IN MUNICIPALITIES LOCATED IN RISK REGIONS:

i. Atypical operation in municipalities located in border regions;
ii. Atypical operation in municipalities located in other regions of landowner, environmental and social risk.
iii. Monitoring must include operations and situations that appear to be related to other operations and related situations or that are part of the same group of operations.

V - BUYING OR SELLING GOLD, OR OTHER PRECIOUS METALS:

I. Operations carried out with legal entities whose representative is a PEP, accounts opened through the attorney-in-fact, residents abroad and the border region will be identified for a specific analysis, focusing on risk and from the perspective of preventing money laundering and terrorist financing, as well as verifying the origin of the funds, presumed financial capacity and the client's tradition in the market. The following will be treated with special attention: (i) payments and receipts made by third parties; (ii) use of financial institutions domiciled in high-risk countries; (iii) divergences between the declared mineral origin and information from official agencies (ANM, environmental agencies); (iv) operations involving countries or counterparties subject to international sanctions; (v) serial operations with values close to any automatic carry-over limits.

VIA BRASIL COMERCIO ATACADISTA DE PRODUTOS DE EXT:39439136000138

Assinado digitalmente por VIA BRASIL COMERCIO ATACADISTA DE PRODUTOS DE EXT:39439136000138
ND: C=BR, CN=VIA BRASIL COMERCIO ATACADISTA DE PRODUTOS DE EXT:39439136000138, L=SAO PAULO, O=ICP-Brasil, OU=videoconferencia, ST=SP
Razão:
Localização:
Data: 2026.06.19 11:14:13-04'00'
Foxit PDF Reader Versão: 2025.3.0