AMSF AUTORITÉ MONÉGASQUE DE SÉCURITÉ FINANCIÈRE

Guideline :

Private banking and wealth management

and

Anti-money laundering, terrorist and proliferation financing

AMSF AUTORITÉ MONÉGASQUE DE SÉCURITÉ FINANCIÈRE

Summary

I. Introduction

The purpose of this guideline is to assist financial institutions in understanding risks associated with Private Banking and Wealth Management and applicable AML/CFT obligations. The guidance contained in this document should be applied risk-based and proportionate, considering the size, nature, and complexity of the business of each financial institution. This guideline does not intend to replace the generic guidelines but to address specific risks and obligations related to Private banking and Asset Management Services separately while not neglecting the broader AML/CFT considerations outlined in the AML/CFT law and other Guidelines. For comprehensive guidance on overall AML/CFT obligations in Monaco, entities should continue to refer to the AMSF "Generic Guidelines for Monegasque Businesses" 2021 (https://amsf.mc/accompagnement/lignes-directrices-et-guides-pratiques)

This Guideline considers standards and guidance issued by the Financial Action Task Force ("FATF"), industry best practices, and red flag indicators identified by the FATF. These are not exhaustive and do not restrict supervised entities' actions to fulfil their legal obligations within the current legal and regulatory framework. In light of their nature, size, and complexity, supervised entities should assess how best to fulfil their legal obligations.

The scope of this Guideline is purely informative. The only legally binding documents are the legislative and regulatory texts governing the anti-money laundering, counter-terrorism and proliferation financing, and corruption framework in Monaco. All obligations and their details are therefore not addressed herein: solely applying the measures presented in this Guideline does not ensure that the institution fully complies with current legal obligations.

The relevant legal provisions relating to the AML/CFT obligations addressed in this guidance are defined in Law no. 1.362 on countering ML, TF, PF and corruption ("the AML/CFT-P Law"), and Sovereign Order no. 2.318. More specifically:

- articles 3 and 3-1 of the Law no 1.362 on countering ML, TF and corruption regarding the obligation to conduct Business Risk Assessment;
- articles 4, 4-3 of the Law no 1.362 on countering ML, TF, PF and corruption and Chapters II et VIII of Sovereign Order no. 2.318 apply to Customer Risk Assessment as well as CDD and EDD Requirements.

Compliance with current legal and regulatory obligations, based on the specific risks it faces, is the responsibility of each obliged entity. This guideline takes into account the regulations in force as of **September 30, 2023**.

II. Context

Professionals active in private banking and wealth management are among the entities subject to AML/CFT-P obligations, as stipulated in the provisions of points 1°) and 3°) of Article 1 of Law No. 1.362 of August 9, 2009, amended.

III. Sectorial risks

Financial Services encompass various financial products and services associated with different ML/TF risks. Private banking is defined as investment services to manage customers' wealth[1]. While these specialized services are attractive to legitimate customers with substantial assets and relatively complex financial affairs, they often have characteristics that are attractive to criminals with significant funds to launder money. Private banking and asset management may be used for layering or integration[2]. FATF defines that Private banking accounts can be attractive to money launderers, particularly those wishing to launder the proceeds of corruption, because of the high net worth of the customer, the offshore nature of many of the facilities offered, and the type of products and services available. These services will likely attract money launderers looking for adequate ventures to move large sums of money without notice. FATF also refers to the reporting institution's desire for a lucrative business relationship with high net-worth individuals, which may make it difficult for compliance officers to convince their boards to turn down dubious customers due to the business's profitability[3].

[1] FATF Guidance for a Risk-Based Approach for the Banking Sector, 2004
[2] BIS AML and CFT in Banking AML and CFT in banking – Executive Summary (bis.org)
[3] FATF Report Specific Risks Factors in Laundering the Proceeds of Corruption. 2012

Exposure of banks and asset management companies to layering and integration is due to the following factors:

ML/TF Risks Associated with Private Banking/Wealth Management

- **Culture of Confidentiality** – the culture of confidentiality in wealth management remains attractive to potential money launderers. Additionally, clients may be reluctant or unwilling to provide adequate documents, details, and explanations.
- **Complex Structures -** The use of services such as offshore trusts and the availability of structures such as shell companies in some jurisdictions helps to maintain an element of secrecy about beneficial ownership of funds and may give rise to significant misuse
- **Complexity of Products and Services** - The inherent complexity of some products and schemes used to serve clients increases ML risks.
- **High-Value Transactions** - The transfer of funds and other assets by customers may involve high-value transactions and rapid transfers of wealth across accounts in different countries and regions of the world; this could facilitate the concealment of illicit funds before the authorities can catch up with them
- **Involvement of Multiple Jurisdictions -** The international nature of private banking increases the likelihood of dealing with illicit proceeds from predicate offenses committed in foreign jurisdictions.
- **PEPs and Risks associated with Corruption** - there are jurisdictions where corruption is known, or perceived, to be a common method of acquiring personal wealth**.**

1. Overview of the Private Banking/Wealth Management Services in Monaco

Private Banks and Asset Management Companies offer private banking/wealth management services in Monaco. ML risks related to private banking and wealth management in Monaco mainly originate from external threats due to the proportion of internationally oriented financial activities. Private banks offer the following types of products to their private banking clientele:

- Investment products
- Reception and transmission of orders
- Current accounts
- Discretionary management services
- Offshore fund management services
- Provision of Advice
- Insurance Services

Asset Management Companies offer mainly discretionary management services, reception and transmission of orders, and provision of advice. The main vulnerabilities identified in the area of private banking and asset management in Monaco are:

- A large percentage of foreign nationals as part of the private bank clientele
- Relatively large amount of International Wire Transfers

2. AMSF Expectations

Considering the unique characteristics of Private banking /wealth management services and associated ML/TF risks, Private Banks and Asset Management Companies are expected to have:

AMSF Expectation related to compliance to AML/CFT Obligations by Private Banks and Asset Management Companies

- Adequate Business Risk Assessment that corresponds to the size, nature, and business profile of the entity;
- Customer Risk Assessment;
- Internal Policies and Procedures aligned with AML/CFT obligations;
- Robust customer due diligence (including identification and verification of Ultimate Beneficial Owners, complex structures, and legal arrangements);
- Enhanced due diligence measures for customers posing high risk;
- Ongoing monitoring of Customer Relationships and update of CDD information on a risk-sensitive basis;
- Adequate transaction monitoring systems that enable entities to identify and report suspicious transactions in a timely manner;
- Adequate systems and controls to manage TF/PF/TFS Risks;
- AML/CFT Training;

IV. Main obligations

Business Risk Assessment

In private banking, conducting a thorough business risk assessment is vital, and should be tailored to the entities' unique products, services, and customer base. Private Banks and Asset Management Companies must ensure that they have a **comprehensive understanding of the ML/TF risks** to which they are exposed. In Conducting Business Risk Assessment, entities shall refer to the AMSF Guidance on Business Risk Assessment (https://amsf.mc/accompagnement/lignes-directrices-et-guides-pratiques).

KEY POINTS : BRA Sound Practices

- Understanding the ML and TF risks to which the entire business is exposed, delineating precise risks pertinent to private banking/asset management, distinct from generic financial services;
- Determining how identified risks are effectively mitigated through internal policies, procedures, and controls;
- Establishing the residual ML/TF risks and any gaps in controls that should be addressed.
- Having a clear risk response strategy that can involve bolstering controls, restricting business relationships, allocating more resources, etc.

The following paragraphs outline specific criteria tailored to private banking and wealth management that should be considered when conducting a Business Risk Assessment. It's important to note that this list is not exhaustive, and the unique circumstances of each business should be thoroughly examined for a comprehensive risk evaluation.

Examples of BRA Risk Factors for Private Banking and Asset Management	
Products, Services Posing Higher Risk	Cash Transactions in large volumes International Wire Transfers Offshore fund management services lending (including mortgages) secured against the value of assets in other jurisdictions
Customer Risk	Ultra-high net wealth individuals PEP's Customers with Complex structure Customers with multi-jurisdictional layers of ownership Holders of bearer shares or other bearer negotiable instruments Legal person customers with nominee shareholders or nominee directors Persons acting as representatives/nominees on behalf of the customer Customers with income and/or wealth from high-risk sectors such as arms, the extractive industries, construction, gambling, or private military contractors Customers with High proportion of Virtual assets as source of Wealth
Delivery Channel Risk	Internet Banking Hold mail Mobile Banking Use of introducers, intermediaries, and/or agents Non-face-to-face onboarding of customer
Geographic Risk	Countries subject to sanctions – TF and PF FATF blacklisted/grey-listed countries Offshore jurisdictions Tax non-compliant jurisdictions Countries associated with high levels of corruption or organized crime
Transaction Risk	Loans intended to be transferred in foreign jurisdictions (Especially Offshore Jurisdictions/Jurisdictions with high Corruption Risks) Transactions involving several intermediaries in multiple Jurisdictions Transactions related to Virtual Currencies Transactions incoming/outgoing to High-Risk Jurisdictions

Customer Due Diligence (CDD)

A sound private banking and asset management business is centered upon having an effective customer due diligence ("CDD") framework. CDD is a set of comprehensive measures to be applied while onboarding a customer. It encompasses a comprehensive approach to understanding and verifying the customer identity and their ultimate beneficial owners. CDD also aids the entity in the decision-making process.

Key elements of the CDD are:

- **Know Your Customer** – involving the collection and verification of essential information about the customer;
- **Customer Screening** – Screening of customer names (including directors, shareholders, UBOs);
- **Customer Risk Assessment** – understanding the risks associated with each customer to ensure appropriate risk mitigation measures are applied to minimize potential threats.
- **Ongoing Monitoring** - CDD is an ongoing process throughout the business relationship. Ongoing monitoring helps detect any suspicious activity and ensure the customer's profile is current. This includes monitoring of customer transactions, changes in the customer's profile, and periodic reviews of customer information.

Based on a holistic view of the information obtained in the context of their application of CDD measures, Private banks, and Asset Management companies should be able to prepare a **customer risk profile.**

CDD also applies to all relevant parties: directors, nominees, shareholders, beneficial owners, intermediaries, and holders of a Power of Attorney (PoA). If the entity relies on a third party, specific risks associated with the third party's jurisdiction shall be assessed.

Customer risk assessment

Customer risk assessment is vital to a sound AML/CFT risk management system. Customer risk assessment forms part of the risk-based approach. Customer Risk Assessment allows entities to assess and categorize clients based on the level of risk they pose concerning ML/TF. By understanding the risk associated with each customer, entities can apply relevant due diligence measures. This allows entities to appropriate due diligence efforts optimizing resource allocation.

Customer Risk Assessment includes considering the risk factors that expose businesses to ML/TF risks.

Utilizing technology for customer risk assessment is optimal, yet smaller institutions can conduct manual assessments effectively. The key lies in ensuring that manual assessments are sophisticated, encompassing all pertinent risk factors and utilizing a robust risk assessment methodology. Regardless of the method, the priority is a comprehensive and accurate evaluation of customer risk for sound risk management practices.

KEY POINTS

- The level of risk linked to every customer dictates the pertinent due diligence measures;
- Irrespective of the approach used, the risk criteria must be relevant and the methodology sound.

Enhanced Due Diligence (EDD)

Due to specific risks applicable to Monaco Private Banking and Asset Management companies, Private Banks and Asset Management Companies are expected to identify high-risk situations and effectively apply EDD measures.

EDD is applicable to high-risk customers determined based on the entity's customer risk assessment. The EDD is a step further in collecting, reviewing, and understanding additional data on a customer to establish a reasonable customer profile. EDD goes beyond CDD and requires more specialized knowledge and investigative skills. It shall be noted that EDD is not a set of measures that substitutes customer due diligence. EDD is applied in addition to Customer Due Diligence.

Key Elements of EDD

- Obtaining additional information on the customer;
- Obtaining additional information on the intended nature of the business relationship and on the reasons for intended or performed transactions;
- Obtaining information on the source of funds or source of wealth of the customer;
- Conduct enhanced monitoring of the business relationship, potentially by increasing the number and timing of controls applied and identifying patterns of transactions that warrant additional scrutiny;
- Applying additional measures for senior management approval, introducing certain limitations on business relationships, etc;

Obtaining information and Documents on the Source of Wealth and Source of Funds is very important for customers subject to Private Banking and Asset Management Services. Entities shall not consider that source of funds and source of wealth information is a similar concept and shall request information and documents in relation to the source of funds and source of wealth separately. Although minor discrepancies in the timeline of wealth accumulation are typical, substantial gaps or noteworthy inconsistencies can pose difficulties in establishing credibility. In such instances, a financial institution may opt to seek additional clarification from the customer. This might involve requesting supplementary documentation or initiating independent inquiries to ensure a more thorough understanding.

Definitions	Applicable Requirements
Source of Wealth describes the activities that have generated the customer's or beneficial owner's total wealth both within and outside a business relationship.	**Understand** a broad picture of the Customer's total wealth and how such wealth was acquired over time (information can be directly obtained from a customer or obtained via public sources). **Request** Documentary Evidence to ensure consistency of information provided by the customer, where there are doubts about its veracity, or where the risks are higher (e.g., PEP from Jurisdiction with high corruption risks.). **Assess** the legitimacy and reasonableness of customer's wealth. **Documentary Evidence Examples:** ▪ Information from a reliable public or private third-party source ▪ Information from financial statements that have been prepared and audited in accordance with generally accepted accounting principles; ▪ Documents issued by a government Authority or a court or local authorities; ▪ Documents issued by entities/professionals subject to AML/CFT supervision. Source of Wealth can be, for example, generated from: **Family/Generational Wealth** inheritance, gifts (from family, including spouse/partner), divorce settlement, lawsuit settlement, pension or retirement benefit scheme pay-outs. **Income, Revenue, and Business Activities** Business ownership, business operations, employment, sales of products, business properties, and other commercial assets. **Investment Activities** income from acquiring and selling investments, e.g., real estate, securities, royalties, patents, inventions and franchises, and virtual assets.
Source of Funds refers to the activity that generated the particular funds for a business relationship or occasional transaction	**Establish** the origin of funds or the reason for the funds having been acquired. Establishing the origin of funds should not be limited to knowing from which financial institution the funds may have been transferred. **Assess**, on an ongoing basis, whether the transactional activity of a business relationship is consistent with the customer's profile, the nature of the product provided, and the entity's understanding of the customer's and beneficial owner's source of wealth.

Key Components of CDD/EDD information

- Purpose and Anticipated activity of a customer;
- Nature of Customer's Wealth and Business;
- Corporate Structure of the Customer;
- Type of products and services to be used;
- Current source of funds for the account;
- Geographic location and jurisdiction of the ownership structure and Ultimate Beneficial ownership;
- References or other information to confirm the reputation of the client.

FIs should assess the reasonableness of relying on self-declarations made by customers regarding the source of funds and wealth. The decision to request specific documents should be risk-based, considering factors such as the customer being a Politically Exposed Person (PEP), originating from a high-risk jurisdiction, or involvement in other high-risk scenarios. In cases of elevated risk, requesting additional documentation becomes necessary. Additionally, it would not suffice to accept information provided by a customer or beneficial owner on an application form without further scrutiny, especially when vague answers are given. For instance, generic responses like 'employment' or 'salary' should be clarified. The supervised entity is urged to verify the source of funds and wealth, particularly in high-value transactions or high-risk relationships, by understanding the customer or beneficial owner's employment details and income.

The obligation to establish the source of funds and wealth extends beyond the initial phase of a business relationship. Ongoing monitoring should include assessing whether the transactional activity aligns with the risk profile, product nature, and the supervised entity's understanding of the customer's and beneficial owner's source of wealth.

FIs are required to maintain a Know Your Customer (KYC) file for each customer. This file serves as a record of customer information and analyses conducted by compliance teams. The KYC file plays a crucial role in demonstrating the extent of scrutiny applied to the customer, including assessments of the source of funds and wealth. Additionally, it documents actions taken to address any identified negative media associated with the customer.

Ongoing CDD

CDD and EDD are not static and include understanding the customer's background, source of wealth, and transactional behavior on an ongoing basis. It also requires a continuous adjustment of the customer profile based on additional information emanating from the transactional and overall customer behavior and new data arising during the relationship. Private Banks and Asset Management companies are expected to perform **CDD reviews** on a risk-sensitive basis, reviewing higher-risk clients at least annually.

Given the risk associated with wealth management activities, it is appropriate that there should be a heightened ongoing review of customers' account activity. The triggers for alerts may be set at different levels depending on the risk the client presents to the business to reflect the appropriate level of control that is to be exercised. Entities using automatic solutions for transaction monitoring shall calibrate their monitoring parameters and alert thresholds to distinguish higher-risk customers and PEPs from other normal business relationships. Entities shall have in place a process to review the monitoring thresholds and parameters on a regular basis to ensure they remain relevant to the institution's risk and customer profile.

FIs should regularly review their automatic transaction monitoring tools to ensure their capability to detect suspicious activities. This involves assessing the effectiveness of the built-in scenarios within these tools. FIs should also evaluate whether the resources allocated for reviewing transactions generated by these systems are sufficient, considering the entity's size and complexity. In cases where tools are used at a group level, it is crucial to ensure that they address the specific vulnerabilities and risks associated with Monaco specifically. When monitoring tools are implemented at a group level, it is essential to guarantee that FIs operating in Monaco have complete access to customer data within these tools. This ensures that customer risk assessments are comprehensive and accurate, containing all the necessary information for a thorough evaluation.

Private Banks and Asset management companies shall have in place processes to ensure that suspicious transaction reports are identified and reported without undue delay.

KEY POINTS

- CDD must be maintained through periodic risk-based reviews;
- Obliged entities must implement, and regularly audit, a transaction monitoring system, adapted to risks;
- Obliged entities must regularly review the transaction monitoring system's effectiveness and ensuring the specific local vulnerabilities and risks are targeted;
- If an obliged entity is part of a group, its access to the systems and information must not be impeded. These issues may be addressed in service agreements.

Illustrative Examples When EDD Shall be Applied

Application of EDD measures is subject to AML/CFT statutory requirements defined under the AML/CFT law of Monaco, Ordinance, and Supervisory Guidance. In addition, entities are authorized to determine additional high-risk categories for which the EDD measures will apply.

Politically Exposed Persons (PEP)

PEPs, or persons related to or associated with PEPs, are particularly important in private banking. PEPs should be treated as customers who potentially pose a higher risk due to their potential power and easier access to public funds. Due to their position and influence, it is recognized that many PEPs are in positions that potentially can be abused for the purpose of committing money laundering offenses and related predicate offenses, including corruption and bribery, as well as conducting activity related to terrorist financing.[4] Where a PEP also has connections to countries or business sectors where corruption is widespread, the risk is further increased.

The nature of the measures applied shall be commensurate with the type of PEP, the identified risks, and the PEP's position and ability to influence.

[4] FATF Guidance Politically Exposed Persons, 2011

Sound practices in PEP Risk Management

- Risk management systems in place to determine whether a customer or BO is a PEP;
- Screening of Customers for PEPs as part of the onboarding process;
- PEP customers are categorized as high-risk in accordance with the entity's Customer Risk Assessment;
- PEP onboarding is subject to senior management approval;
- Periodic Screening of Existing Customer Base;
- EDD is applied to family members and close associates of PEPs.

For more information regarding PEPs, please refer to the topical Guideline (https://amsf.mc/accompagnement/lignes-directrices-et-guides-pratiques).

Complex structures

Usually, legal structures private banking/wealth management customers use are complex regarding the layers of ownership and the legal entities and arrangements used. Intricate ownership structures require further scrutiny. Private banks and Asset Management companies must thoroughly comprehend these complex setups to ensure that they fully understand the ownership chain and are able to identify and verify who the ultimate beneficial owner is.

Using services such as offshore trusts and the availability of structures such as shell companies in some jurisdictions helps maintain an element of secrecy about beneficial ownership of funds and may give rise to significant misuse. Therefore, Private banks and Asset Management companies are expected to understand the reasons and purpose for their customers' structures. They should assess the legitimacy of such structures, especially those involving multiple layers of offshore holding companies. Where trust structures are used, entities should identify and document the ultimate settlor/beneficiary/protector/beneficial owner of the assets/funds underlying the trust structures, which should be a natural person.

KEY POINTS

- Complex structures must undergo additional analysis to clarify the underlying economic reasons and purposes as well as identify the BOs;
- Any service, exposed to the risk of abuse, must be taken into account to fully comprehend the validity of the chosen structure.

AML/CFT training

AML/CFT training is a key element of sound ML/TF risk management system. Since private bankers have close interactions and a deep understanding of clients, providing thorough training on AML/CFT matters is critical to ensure that risks are managed adequately. Front-line staff in private banking should be well trained and specialize in CDD/EDD, identification of suspicious activities, and recognizing red flags. The specialized training should emphasize the unique risk factors within private banking, such as complex ownership structures and high transaction volumes. Training should cover overall AML/CFT regulatory requirements, supervisory guidance, and the entity's internal AML/CFT policies, procedures, and processes. Training should be tailored to each individual's specific responsibilities, as appropriate.

Sound Practices for Effective AML/CFT Training Program

- First and Second Line responsibilities are explained in detail;
- Clear Guidelines of What constitutes SoF/SoW and type of documents can be obtained from customers;
- Training provides a description of Suspicious Transaction Red Flags and Scenarios;
- Tailored training is in place to ensure that employees' technical knowledge is adequate and current. Employees have easy access to policies and procedures;
- Training covers practical examples, uses case studies, and provides information on policy compliance;
- Implement a mechanism to assess individual training needs, such as a form of testing on completion for example;
- The entity maintains records of all training.

V. Red flags scenarios for Private Banking and Asset Management

An illustrative (but not exhaustive) list of Red Flag Scenarios for Private Banking and Asset Management	
Red Flags Associated with Source of Wealth	Customers whose bulk of source of wealth is derived from investments in virtual assets. Customer's source of wealth is disproportionately drawn from virtual assets originating from other virtual asset service providers that lack anti-money laundering or counter-terrorist financing controls. The customer's funds originate from or are sent to, an exchange that is not registered in the jurisdiction where either the customer or exchange is located.
Red Flags for Private Banking and Asset Management Based on information gathered through the CDD/EDD Process	Not Clear Information regarding the Business and Profile of the Customer. Account opened for nonresidents without documentary evidence for the source of wealth. Account for HNWIs with third-party power of attorney (POA) operation. Business account for HNWIs with multilayer ownership structure, third-party POA. Offshore entities located in jurisdictions with weak AML regimes. Accounts for Operational Companies. Legal structure is set-up in the jurisdiction not subject to FATCA/CRS reporting obligations. Use of companies or legal structures located in a jurisdiction other than the tax residence or place of regular economic or professional interest of the UBOs. Complex setup without specific economic rationale. Customer is not interested in earning a return.
Red Flags Based on Transaction Monitoring	Transactions related to high-risk jurisdictions. Transactions without legitimate economic rationale. Frequent payment for Fees related to Marketing or other types of services which are difficult to verify. Customer uses cash intensively. Transactions linked to commercial activities through private accounts. Frequent incoming/outgoing transactions to/from jurisdictions without legitimate commercial purpose. No Clear information on the incoming source of funds is provided by the customer.

VI. Case study

Facts :

A client from another entity within a group to which a Monégasque bank belongs wishes to open an account in this subsidiary, despite having no ties to the Principality (such as nationality, residence, family, economic interests or real estate).

Highly affluent, Mr. Z seeks to open a personal account with a wealth management focus, intending to invest in the stock market.

Mr. Z plans to carry out investment operations as follows: funds, originating from loan agreements, are intended for six companies registered in Cyprus, amounting to a total of 175 million Euros, through 6 distinct transactions, executed via wire transfer. The Cypriot companies will, in turn, be responsible for executing the investment orders.

According to the legal documentation provided, all six Cypriot companies are recently founded, having been established within a span of two months.

Upon analyzing the provided legal documentation, it appears two politically exposed persons (PEP), listed on the national freeze list of an Easter Europe country, are among the beneficial owners of these structures. Additionally, one of the beneficial owners is also subject to adverse media; several press articles allege fraudulent bankruptcy.

Mr. Z expresses a desire to conduct similar operations periodically, in the near future.

The indicators to be analyzed are as follows:

- **Opening an account without ties to the Principality of Monaco** :

It is essential to precisely determine the reasons for opening this account and ensure that the objective is not to negatively exploit the local financial system.

- **Stock Market Investments via Loans:**

Investment operations in the stock market involving funds originating from loan agreements raise questions about their source. It is necessary to establish their legality, especially considering the substantial cumulative amounts.

- **Use of structures**:

The use of newly created intermediary companies in a jurisdiction, with no ties to the final beneficial owner, may suggest an intent to obscure, complicate or conceal transactions. The reasons behind this arrangement require clarification.

- **Politically Exposed Persons (PEP) and/or those associated with negative information:**

The involvement of PEPs, listed on a national freeze list and/or associated with negative information, including allegations of fraudulent bankruptcy, are higher risk criteria which are necessary to assess the transactions' risk profile. Enhanced monitoring may therefore be required.

- **Renewal of such operations:**

After carefully reviewing whether the account functions as expected and is consistent with customer knowledge, the risks associated with these operations may indicate a need for continuous and heightened account monitoring.

Overall, the described scenario requires a thorough evaluation by the bank to understand the transactions' economic rationale and ensure it is consistent with customer due diligence and risk profile.