White Paper in the Management of Blocked Accounts

by the LPEA AML/CFT Committee

May 2025

About LPEA

The Luxembourg Private Equity and Venture Capital Association ("**LPEA**") aims at promoting and defending the interests of investors and professionals principally active in the field of Private Equity ("**PE**") and Venture Capital ("**VC**").

The Association is the trusted and relevant representative body of PE and VC practitioners with a presence in Luxembourg.

Created in 2010 by a leading group of PE and VC players, with more than 600 members, LPEA plays a leading role locally, actively promoting PE and VC in Luxembourg.

LPEA provides a dynamic and interactive platform, which helps investors and advisors to navigate through latest trends in the industry. International by nature, the association allows members to network, exchange experience, expand their knowledge and grow professionally attending workshops and trainings held on a regular basis.

About the document

The work presented herein is issued on behalf of the members of the LPEA AML Expert Working Group (the "**Working Group**"), who are professionals active in the field of anti-money laundering ("**AML**") and counter-terrorism financing ("**CTF**"). This White Paper was prepared as an outcome of a Transfer Agents ("**TA**") Roundtable organized on May 14, 2024. The Association maintains a neutral stance regarding the insights shared within this context. The LPEA does not provide specific advice or endorse any particular company, product, or service over another.

This document is for general information purposes only and might be amended from time to time. Although care has been taken in drawing it up, it does not constitute advice or official guidance and should therefore not be relied upon or used as such. Neither the LPEA nor any of its working groups, committees or members accepts any responsibility or liability for damages arising out of the use of this document.

Introduction

The Luxembourg financial market operates under a rigorous regulatory framework designed to ensure transparency, security and compliance in all financial transactions. One critical aspect of this framework is the practice related to the management of blocked accounts, including the initiation thereof as well as the remediation.

This document sets out arrangements that firms could consider to ensure adequate controls are in place in relation to the management of blocked accounts.

Outcome of the TA Roundtable

The TA Roundtable conducted on May 14, 2024 has shown high interest of market participants in aligning internal procedures with standard market practice.

This document reflects the outcome of the TA Roundtable and demonstrates participants' mutual wish to highlight synergies and efficiencies in the processes pertaining to blocked accounts.

- Half of the participants answered that the blocking reasons are defined by internal procedure and tool configurations.
- Reasons for blocked accounts are either defined by a drop down list or manually.
- Top 3 reasons for blocking of accounts are: missing KYC, ML/TF suspicious and requests from the Financial Intelligence Unit ("FIU").
- Service level agreement would in most cases cover transaction monitoring processes, but not specifically obligations related to goAML filings.
- Half of the participants answered that they do not report SAR/STR filed to the Client/Fund as they consider that it would constitute a tipping-off.
- Most participants would freeze accounts immediately after receiving a sanctions hit on the entity or person and would immediately escalate to the Client/Fund.
- In case of a hit on the OFAC/UK sanctions list, only half of the respondents would file a SAR/STR.

Based on aforementioned responses, several best practices can be identified:

1. **Standardized labeling systems:** Financial institutions may want to implement a standardized labeling system to categorize blocked accounts. This system could include distinct labels that clearly indicate the reason for blocking. Suggested labels may include:
   - **AML Blocking reasons:**
     - **AML-Suspicion**: For accounts blocked due to suspicious activities that may indicate money laundering, a predicate offence thereof or terrorist financing. Such may include reluctance to provide information related to the identification and verification of UBOs.
     - **Sanctions**: Freezing of accounts due to results from the implementation of a targeted financial sanction ("TFS") regime.
   - **Other blocking reasons:**
     - **Operational**: For accounts blocked due to operational reasons (e.g. transfer out, migration, liquidation, or death of the account holder).

- **Other documentation missing**: For accounts where originals of KYC documents are missing or material[1] KYC is missing for already identified and verified UBOs (in cases of periodic due diligence or trigger event).

2. Detailed documentation: Financial institutions may want to establish, for each blocked account, a detailed documented assessment explaining the reason for the blocking. This documentation may include:

- **Reason for blocking**: A clear explanation of the reason why the account was blocked, referencing relevant laws, regulations or internal policies.
- **Type of blocking**: full or partial.
- **Date of blocking**: The date when the account was blocked.
- **Authority**: The name and title of the person or department that authorized the blocking.
- **Supporting evidence**: Any evidence or documentation supporting the decision to block the account (e.g. transaction reports, customer communications) including remediation and unblocking process (date of the last/next chaser to the customer/investor, date of the last/next review of the blocking status, etc.).
- **Labeling assigned to the type of blocking**: AML-related blocking reason or non-AML-related blocking reason.

3. Monitoring and review: Financial institutions may want to conduct regular monitoring and review of blocked accounts to ensure accuracy and compliance. This process may include:

- **Periodic reviews**: Scheduled reviews of blocked accounts to reassess the reasons for blocking and to ensure that accounts are not unnecessarily blocked for extended periods of time.
- **Internal audits**: Regular internal audits to verify that the labeling and documentation of blocked accounts comply with the institution's AML policies and regulatory requirements.
- **Updates and adjustments**: Updating account labels and documentation as new information becomes available or as the status of the account changes.

4. Staff training: Financial institutions may want to provide to all relevant staff training on the standardized labeling system and the importance of accurate documentation. Training may notably cover:

- **AML regulations**: Key AML regulations and the institution's internal policies regarding blocked accounts.
- **Labeling procedures**: Procedures for accurately labeling and documenting blocked accounts.
- **Reporting requirements**: Requirements for reporting suspicious activities and maintaining records.

5. Reporting and communication: Financial institutions may want to establish clear communication channels for reporting and discussing blocked accounts, particularly those blocked for AML reasons. This may notably include:

- **Internal reporting**: Procedures for internal reporting of suspicious activities, transactions and blocked accounts to the compliance department.

[1] *"Material KYC for already identified and verified UBOs" refers to the core identification and verification documents and typically include official identification documents, evidence of ownership/control structure, and, where relevant, documentation on the source of wealth.*

- **External reporting**: Requirements for reporting suspicious activities and transactions to relevant authorities, such as the *Cellule de Renseignement Financier* ("**CRF**"), Luxembourg's FIU, including implementation of a TFS regime to the Ministry of Finance of Luxembourg (and parallel reporting to the relevant competent authority)
- **Client communication**: Guidance for communicating with clients about the status of their blocked accounts, ensuring transparency while complying with legal restrictions on disclosure.

6. Non-tipping off and dissemination of information between obliged entities: Financial institutions may want to ensure a clear understanding related to no-tipping-off rules which should be part of their internal policies. As stipulated in the AML Directive IV, several disclosures related to the submission of a SAR/STR are protected from the applicability of the no-tipping-off rules. As reflected in Article 39 of the AML Directive IV, the prohibition to disclose information is related solely to a Client being a third party to contractual relationships between the TA and the Fund/GP/AIFM. Furthermore and additionally, as per Article 5 (5) of the AML Law, Luxembourg TAs may have a basis to disclose to Luxembourg IFMs/Funds information, in cases involving the same person concerned and the same transaction in relation to whom they filed a SAR, when such disclosure is performed exclusively for the purposes of the prevention of money laundering and terrorist financing.

7. Concluding remarks:

- It is important to highlight that each obliged entity is solely and fully responsible for compliance with Article 5 of the AML Law 2004 as amended in relation to cooperation with Authorities. Limited reliance should be placed on any service provider regardless of any service level agreement – while the latter can contribute to the cooperation between such service provider and the obliged entity, it would never replace the responsibility of the latter.
- It is highly advisable that obliged entities subject to AML Law and supervision by relevant supervisory authorities should clearly distinguish between AML-related blocking and non-AML-related blocking. Appropriate classification is subject to entities' internal AML/CFT policies, Group policies if applicable, as well as IT systems used for client registration.

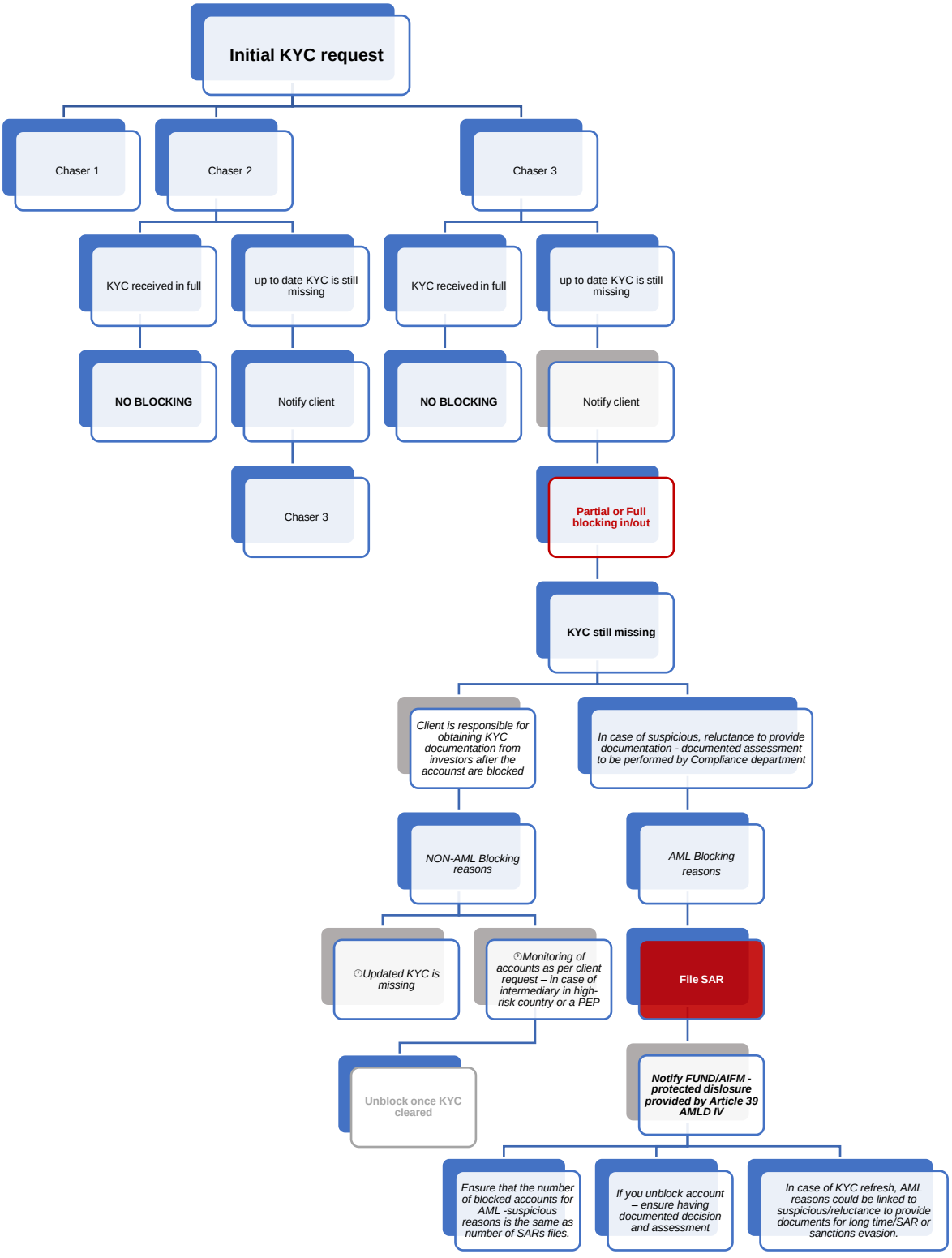
Main sources of information

- *Ministry of Finance, Guidelines Relating to the implementation of financial restrictive measures (sanctions)1 against third countries, entities or individuals: Guide de bonne conduite_Sanctions financières Non-TF_EN (gouvernement.lu)*
- *CSSF, Law of 12 November 2004 (coordinated version): Law of 12 November 2004 on the fight against money laundering and terrorist financing (cssf.lu)*
- *CSSF, CSSF Regulation 12-02 as amended: CSSF Regulation No 12-02 of 14 December 2012 on the fight against money laundering and terrorist financing*
- *CRF, Suspicious operations report Guideline applicable from 01.04.202: Suspicious operations report - Guideline applicable from 01.04.2021 (public.lu)*
- *Law of 19 December 2020 on the implementation of restrictive measures in financial matters, as amended: https://www.cssf.lu/wp-content/uploads/L_191220_restrictive_measures_eng.pdf*
- *Guidelines of the Ministry of Finance relating to the implementation of financial sanctions against certain persons, entities, bodies and groups within the framework of combating terrorism financing: https://mfin.gouvernement.lu/dam-assets/dossiers/sanctions-financi%C3%A8res-internationales/documentation/guides-2024/1-guide-de-bonne-conduite-sanctions-financieres-tf-en.pdf*
- *CRF, Freezing of suspicious transactions guideline applicable from 01/04/2021: https://justice.public.lu/content/dam/justice/fr/legislation/circulaires/crf-lignedirectriceblocages/2021-04-01-freezing-of-suspicious-transactions-version-2-1.pdf*
- *AED guidelines, such as technical sheet on TFS (https://pfi.public.lu/content/dam/pfi/pdf/blanchiment/sanctions/fiche-technique-relative-aux-sanctions-financires-internationales.pdf), Guide on AML/CFT professional obligations for RAIFs (https://pfi.public.lu/content/dam/pfi/blanchiment/2023/engl/mars/guide-version-032023-raif.pdf)*
- *DIRECTIVE (EU) 2015/ 849 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL - of 20 May 2015 - on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing, amending Regulation (EU) No 648/ 2012 of the European Parliament and of the Council, and repealing Directive 2005/ 60/ EC of the European Parliament and of the Council and Commission Directive 2006/ 70/ EC*

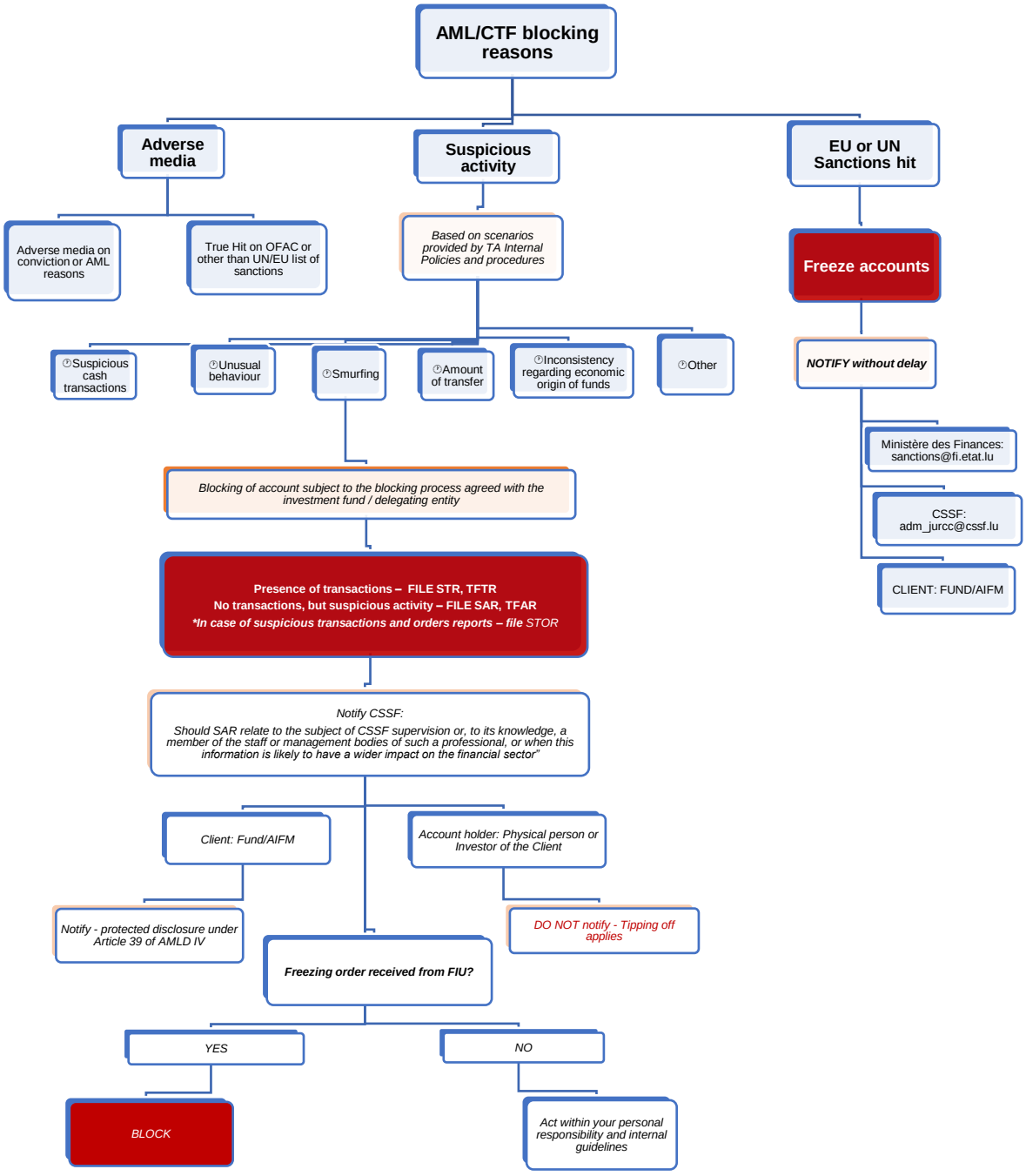
Appendix: Cases

Below cases reflect two different, indicative scenarios that financial institutions may want to consider in the context of blocked accounts' management.

Case 1: Periodic Due Diligence process



Case 2: AML/CTF reasons other than KYC missing.



LPEA