AMENDMENTS No. 1

Practical Guidance to AIFC Anti-Money Laundering and Counter – Terrorist Financing Framework

Approval date: 19 December 2024

Commencement date: 1 January 2025

Astana, Kazakhstan

Within the amendments to the AIFC AML/CFT framework

In this Practical Guidance, the underlining indicates a new text and the strikethrough indicates a removed text

(…)

Revision history

Version	Date	Change description	Section changed
AMLPG 001	15/04/2022	n/a	n/a
AMLPG 002		Amendments on AML audit.	Annex 7
AMLPG 003	______________ 2024	Amendments consequential to amendments to the AML Rules	Part 3 Part 4 Part 5 Part 6 Part 8 Part 9 Annex 1 Annex 2 Annex 7

(…)

Version	**Date**	**Part 3**	
AMLPG 003~~1~~	~~15~~__/__~~04~~/202~~2~~4	**Risk-Based Approach**	s. 3.1 – 3.21
		▪ *Business risk assessment*	s. 3.4 – 3.7
		▪ *Considering relevant risk factors*	s. 3.8 – 3.10
		▪ *Keeping risk assessment up-to-date*	s. 3.11
		▪ *Documenting risk assessment*	s. 3.12
		▪ *Obtaining senior management approval*	s. 3.13
		▪ *Group-wide ML/TF risk assessment*	s. 3.14 – 3.15
		▪ *Customer risk assessment*	s. 3.16 – 3.18
		▪ *Conducting customer risk assessment*	s. 3.19 – 3.21

(…)

Subject	3	**RISK-BASED APPROACH**
(…)		
	3.3	Relevant Persons should also assess the ML/TF risks associated with a customer or proposed business relationship (hereafter referred to as "customer risk assessment") to determine the degree, frequency or extent of CDD measures and ongoing monitoring conducted, which should vary in accordance with the assessed ML/TF risks associated with the customer or business relationship.

		The general idea is that, for instance, if the scale is from 1 to 10, then 10 will correspond to the highest risk and 1 to the lowest (the same logic should be if the scale will be from 1 to 100). Individual categories can be scored: 1–3 as lower risk, 4–7 medium risk, and 8–10 as high risk. These risk categories are then combined to produce a composite score. If the result exceeds the highest grade, it should be considered as prohibited, extremely high (intolerable). A simple model simply adds up the category totals, resulting in a score ranging. The model can be made more complex by weighting each of the factors and subfactors differently, for example by focusing more on customer type rather than to product or country. The model can be made even more complex, for example by creating combinations of factors that will determine the overall rating. The degree of complexity varies by organisation; the more complex, the more likely the rating will reflect the real client's overall risk.
AML Rule 4.2		**Business risk assessment (BURA)**
(…)		
AML Rule 4.2.1		**Considering relevant risk factors**
	3.8	A Relevant Person should holistically take into account relevant risk factors including country risk, customer risk, product/service/transaction risk, delivery/distribution channel risk and, where applicable, other risks that the Relevant Person is exposed to, depending on its specific circumstances. While there is no complete set of risk indicators, the list of risk indicators outlined in Annex 1 may help identify a higher or lower level of risk associated with the risk factors stated above that may be present in the business operations of a Relevant Person or its customer base and should be taken into account holistically whenever relevant in the business risk assessment. BURA should also consider: Complexity of business model Industries and target markets Geographic areas of main activity including transactions and customers residence Types of customers Characteristic of products and services in terms of exposure to financial crimes

(…)		
AML Rule 5.1		**Customer risk assessment**
	3.16	A Relevant Person should assess the ML/TF risks associated with a customer or a proposed business relationship and create a customer risk profile. The information obtained in the initial stages of the CDD process should enable a Relevant Person to conduct a customer risk assessment, which would determine the level of CDD measures to be applied. The measures must, however, comply with the legal requirements of the AML Rules. The general principle is that the amount and type of information obtained, and the extent to which this information is verified, should be increased where the risk associated with the business relationship is higher, or may be decreased where the associated risk is lower. Customer risk profile should include documentation of customers intended activities and relationship with the company. The goal is to establish what is normal and expected activity, which forms baseline for monitoring unusual or suspicious activity. Customer risk profile should be created based on the triad – customer's inherent characteristics (demographics like the age, occupation, average income and source of funds/source of wealth), geographic region and products and services they are seeking. An ongoing monitoring should be based on the customer risk profile. Update of the customer risk profile should be performed according to the risk level (the higher risk, the more frequent).
(…)		
	3.20.	Similar to other parts of the AML/CFT Systems, a Relevant Person should adopt an RBA in the design and implementation of its customer risk assessment framework, and the framework should be designed taking into account the results of the business risk assessment of the Relevant Person and commensurate with the risk profile and complexity of its customer base. The customer risk assessment should holistically take into account a customer's relevant risk factors, including the country risk, customer risk, product/service/transaction risk, and delivery/distribution channel risk, patterns of unusual behavior. Unusual behaviour of the customer is a behaviour that contradicts with expected activity of the customer based on available data. (For example, it may include inconsistency with the amount of initial capital, deposited funds,

		transactions with the provided source of funds and source of wealth, or inconsistency of the geographical area of transactions with the data provided at the onboarding stage, etc.).

(…)

Version	**Date**	**Part 4**	
AMLPG 00~~1~~3	~~15~~ /~~04~~ /2024~~2~~	**AML/CFT Systems**	s. 4.1 – 4.17
		▪ *Internal control programmes for AML/CFT purposes*	s. 4.2 – 4.2.1
		▪ *Compliance management arrangements*	s. 4.6
		▪ *Senior management oversight*	s. 4.7 – 4.8
		▪ *Compliance officer and money laundering reporting officer*	s. 4.9 – 4.10
		▪ *Independent audit function*	s. 4.11 – 4.12
		▪ *Employee screening*	s. 4.13 – 14.13-1
		▪ *Group-wide AML/CFT Systems*	s. 4.14 – 4.17

Subject	**4**	**AML/CFT SYSTEMS**
(…)		
AML Rule 4.3.1	4.5	Having regard to the nature, size and complexity of its businesses and the ML/TF risks arising from those businesses, a Relevant Person should implement adequate and appropriate policies, procedures, systems and controls which should, at

		minimum, include: (a) appropriate representation of AML compliance function in the managing, organising internal control system on AML matters; (b) risk management programme (BURA, CRA); (c) customer identification programme (KYC/CDD); (d) transaction monitoring and reviewing; (e) employees training and awareness programme; (f) adequate employee screening procedures (Know Your Employees); (g) independent audit to test the system. ~~(a) risk management;~~ ~~(b) customer identification;~~ ~~(c) transaction monitoring and reviewing;~~ ~~(d) compliance management arrangements;~~ ~~(e) independent audit function;~~ ~~(f) employee screening procedures; and~~ ~~(g) an ongoing employee training programme.~~ A Relevant Person may rely on a third party consultant to develop policies, procedures, systems and controls required for the purposes of AML Rule 4.3.1. Such third party consultant must perform its work with skill, care, and diligence and shall possess the following characteristics: 1) relevant knowledge and expertise, confirmed by the certificate from one of the internationally recognised professional organisations (such as ACAMS, ICA, ACFCS or analogy); 2) robust knowledge of the AIFC Acting Law and National AML regulation;

		3) industry specific expertise confirmed by previous consulting experience in the AML/CFT, sanctions compliance field; 4) absence of negative feedback from the AFSA with regard to the work of such third party consultant conducted for other companies. The Relevant Person relying on such a third party shall bear ultimate responsibility for the policies, procedures, systems and controls adopted by the Relevant Person.
(…)		
		Compliance officer (CO) and Money Laundering Reporting Officer (MLRO)
(…)		
Annex 5 – Principal functions expected from a MLRO	4.10	A Relevant Person should appoint an MLRO as a central reference point for reporting suspicious transactions and also as the main point of contact with the FIU and law enforcement agencies. The appointment should be carried out by the relevant decision-making body (or sole decision maker) pursuant to internal corporate arrangements of the Relevant Person. The MLRO should play an active role in identifying and reporting suspicious transactions. Principal functions expected from the MLRO are outlined in Annex 5 and include: (a) implementation of the AML/CFT – related internal controls; (b) carry out analysis of the Relevant Person's operations for AML/CFT purposes; and (c) cooperation with competent authorities. The individual appointed as MLRO needs to avoid conflicts of interest, whether real or potential. Thus the MLRO should not combine the role of the business owner, shareholder or CEO/executive management due to the conflict of duties of second line of defence. A MLRO’s necessary skills and knowledge are outlined in Annex 5.
(…)		
		Employee screening

	4.13	Relevant Persons should have adequate and appropriate screening procedures in order to ensure high standards when hiring employees (Know Your Employee).
	4.13-1	The relevant due diligence procedures should be applied to employees in sensitive roles. This could be background screening, verifying identity, checking criminal records, and references. An employee should be screened through the same lists and sources the company uses for prospective customers (sanctions, PEPs, watchlists, negative information). After on-boarding the new employee should be brought to the compliance culture by inoculating them with the main principles and values from the very beginning. They need to know and agree to abide by the code of conduct, ethics and compliance policy.
(…)		

Version	**Date**	**Part 5**	
AMLPG 00~~1~~3	~~15~~ /~~04~~ /2024~~2~~	**Customer Due Diligence**	s. 5.1 – 5.83
		▪ *What CDD measures are and when they must be carried out*	s. 5.1 – 5.2
		▪ *What CDD measures are*	s. 5.3 – 5.7
		▪ *When CDD measures must be carried out*	s. 5.8 – 5.10
		▪ *Identification and verification of the customer's identity*	s. 5.11
		▪ *Customer that is a natural person*	s. 5.12 – 5.14
		▪ *Customer that is a legal person*	s. 5.15 – 5.18
		▪ *Customer that is a trust or other similar legal arrangement*	s. 5.19 – 5.22
		▪ *Identification and verification of a beneficial owner (BO)*	s. 5.23 – 5.28

		▪ *Beneficial owner in relation to a natural person*	s. 5.29
		▪ *Beneficial owner in relation to a legal person*	s. 5.30
		▪ *Beneficial owner in relation to a Trust*	s. 5.31
		▪ *Ownership and control structure*	s. 5.32 – 5.36
		▪ *Threshold and indirect ownership*	s. 5.37 – 5.38-1
		▪ *Identification and verification of a person named to act on behalf of the customer*	s. 5.39 – 5.44
		▪ *Reliability of documents, data or information*	s. 5.45 – 5.49
		▪ *Purpose and intended nature of business relationship*	s. 5.50 – 5.51
		▪ *Delayed identity verification during the establishment of a business relationship*	s. 5.52 – 5.56
		▪ *Simplified customer due diligence (SDD)*	s. 5.57 – 5.60
		▪ *Listed company*	s. 5.61
		▪ *Government and public body*	s. 5.62 – 5.63
		▪ *Customer not physically present for identification purposes*	s. 5.64
		▪ *Special requirements*	s. 5.65 – 5.68
		▪ *Nominee shareholders*	s. 5.69
		▪ *Jurisdictions posing a higher risk*	s. 5.70 – 5.71
		▪ *Jurisdictions subject to a call by the FATF*	s. 5.72 – 5.73

		▪ *Reliance on CDD performed by third parties*	s. 5.74 – 5.80-1
		▪ *Third parties*	s. 5.81
		▪ *Failure to satisfactorily complete CDD measures*	s. 5.82
		▪ *Prohibition on anonymous accounts*	s. 5.83

Subject	**5**	**CUSTOMER DUE DILIGENCE**
(…)		
		What CDD measures are
	5.4	The following are CDD measures applicable to a Relevant Person: (a) identify the customer and verify the customer's identity using documents, data or information provided by a reliable and independent source (see section 5.11); (b) where there is a beneficial owner in relation to the customer, identify and take reasonable measures to verify the beneficial owner's identity so that the Relevant Person is satisfied that it knows who the beneficial owner is, including, in the case of a legal person or trust, measures to enable the Relevant Person to understand the ownership and control structure of the legal person or trust (see sections 5.23 – 5.44); (c) obtain information on the purpose and intended nature of the business relationship (if any) established with the Relevant Person unless the purpose and intended nature are obvious (see sections 5.50 and 5.51); (d) understand the customer's sources of funds and sources of wealth; and (e) ~~(d)~~ if a person purports to act on behalf of the customer: (i) identify the person and take reasonable measures to verify the person's identity using documents, data or

		information provided by a reliable and independent source; and verify the person's authority to act on behalf of the customer (see sections 5.39 – 5.44).
(…)		
		When CDD measures must be carried out
AML Rule 6.1.1 AML Rule 6.2.1	5.8	A Relevant Person must carry out CDD measures in relation to a customer: (a) at the outset of a business relationship; (b) before performing any occasional transaction: (i) with Digital Assets the value of which singularly or in several linked operations (whether at the time or later), is equal or exceeds USD 1,000; (ii) equal to or exceeding an aggregate value of USD 15,000, whether carried out in a single operation or several operations that appear to the Relevant Person to be linked; or (iii) a wire transfer equal to or exceeding an aggregate value of USD 1,000, whether carried out in a single operation or several operations that appear to the Relevant Person to be linked; (c) when the Relevant Person suspects that the customer or the customer's account is involved in ML/TF; or (d) when the Relevant Person doubts the veracity or adequacy of any information previously obtained for the purpose of identifying the customer or for the purpose of verifying the customer's identity.
	5.9	Relevant Persons should be vigilant to the possibility that a series of linked occasional transactions could meet or exceed the CDD thresholds of USD 1,000 for wire transfers or transactions with Digital Assets and USD 15,000 for other types of transactions. Where Relevant Persons become aware that these thresholds are met or exceeded, CDD measures must be carried out.
(…)		
Guidance on customer due	5.38-	In order to correctly understand the sources of funds and wealth, the Relevant Person should collect information from

diligence	1	the clients themselves, for instance, in the form of a special paper or digital form. This form should allow the client to indicate among others their demographic data, occupation, sources of origin and indicate their approximate average income. It is important to inform the client about the need to indicate the actual volume of existing income, and not the desired one. Depending on the information collected while establishing risk profile of the client, the Relevant Person will be able to establish an understanding of what is usual for the client with this particular set of characteristics and what will go beyond the usual behavior/activity. Thus, characteristics that go beyond the usual behavior should be a criterion that increases the risks of Customer at the CDD stage. In case of increased risks, the EDD procedures should be applied to verify the sources of funds and wealth. The absence of requirement to request additional documented confirmation of the source of funds or wealth in the case of standard CDD should not mislead the Relevant Person into considering that there is no need to apply enhanced verification measures and limit the use of the EDD. The risk-based verification should be applied. In particular the client risk assessment system should stipulate that the Relevant Person, adapting it to the certain characteristics and specifics of the business, determines what is usual (understandable and explainable) and what raises doubts or concerns. Factors that raise doubts or concerns should increase the level of risk and provide for appropriate enhanced measures.
(…)		
		Reliance on CDD performed by third parties
(…)		
	5.80-1	A Relevant Person must not rely on third parties to provide ongoing monitoring CDD procedures. It should be the responsibility of the Relevant Person to conduct ongoing due diligence throughout the course of the business relationship to ensure consistency of the transactions with the Relevant Person's knowledge of the customer, their business and risk profile, including, the source of funds.
(…)		

Version	Date	Part 6	
AMLPG 001	15/04/2022	**Politically Exposed Persons (PEPs)**	s. 6.1 – 6.14
		▪ *General*	s. 6.1 – 6.7
		▪ *Special requirements and additional measures for PEPs*	s. 6.8 – 6.1415

Subject	6	POLITICALLY EXPOSED PERSONS (PEPs)
(…)		
	6.15	According to FATF Recommendation 12 the handling of a person who is no longer entrusted with a prominent public function should be based on an assessment of risk and not on prescribed time limits. The risk based approach requires that financial institutions and DNFBPs assess the ML/TF risk of a PEP who is no longer entrusted with a prominent public function, and take effective action to mitigate this risk. Possible risk factors are: (1) the level of (informal) influence that the individual could still exercise; the seniority of the position that the individual held as a PEP; or (2) whether the individual's previous and current function are linked in any way (e.g., formally by appointment of the PEPs successor, or informally by the fact that the PEP continues to deal with the same substantive matters).

(…)

Version	Date	Part 8	
AMLPG 00~~1~~3	~~15~~__/__~~04~~/202~~2~~4	**Terrorist Financing, Financial Sanctions and Proliferation Financing**	s. 8.1 – 8.12
		▪ *Terrorist financing (TF)*	s. 8.1 – 8.2

		- *Financial sanctions & proliferation financing*	s. 8.3
		- *Sanctions imposed by other jurisdictions*	s. 8.4
		- *Database maintenance, screening and enhanced checking*	s. 8.5 – 8.12

Subject	**8**	**TERRORIST FINANCING, FINANCIAL SANCTIONS AND PROLIFERATION FINANCING**
(…)		
		Sanctions imposed by other jurisdictions
	8.4	A Relevant Person operating internationally will need to be aware of the scope and focus of relevant sanctions regimes in those jurisdictions. Where these sanctions regimes may affect their operations, Relevant Persons should consider what implications exist and take appropriate measures, such as including relevant overseas designations in its database for screening purpose, where applicable. Such regimes include unilateral sanctions imposed by the US (administered by Office of Foreign Assets Control (OFAC)), the European Union (EU), and United Kingdom (administered by His Majesty's Treasury Office of Financial Sanctions Implementation (HMT UK OFSI)).
(…)		

Version	**Date**	**Part 9**	
AMLPG 00~~1~~3	~~15~~__/__~~04~~/2024~~2~~	**Suspicious Transaction Reports, Threshold Transaction Reports and Law Enforcement Requests**	s. 9.1 – 9.35
		- *General issues*	s. 9.1

		▪ *Knowledge vs. suspicion*	s. 9.2 – 9.5
		▪ *Tipping-off*	s. 9.6
		▪ *AML/CFT Systems in relation to suspicious transaction reporting and threshold transaction reporting*	s. 9.7 – 9.8
		▪ *Money laundering reporting officer*	s. 9.9
		▪ *Identifying suspicious transactions*	s. 9.10 – 9.11
		▪ *Internal reporting*	s. 9.12 – 9.18
		▪ *Reporting to the FIU*	s. 9.19 – 9.23
		▪ *Post reporting matters*	s. 9.24 – 9.28
		▪ *Record-keeping*	s. 9.29 – 9.30
		▪ *Requests from law enforcement agencies*	s. 9.31 – 9.35

Subject	**9**	**SUSPICIOUS TRANSACTION REPORTS, THRESHOLD TRANSACTION REPORTS AND LAW ENFORCEMENT REQUESTS**
(…)		
		Knowledge vs. suspicion
(…)		
	9.3	Suspicion is more subjective. Suspicion is personal and falls short of proof based on firm evidence. As far as a Relevant Person is concerned, when a transaction or a series of transactions of a customer is not consistent with the Relevant

		Person’s knowledge of the customer, or is unusual (e.g. in a pattern that has no apparent economic or lawful purpose, or by unnecessary routing of funds through third party accounts), the Relevant Person should take appropriate steps to further examine the transactions and identify if there is any suspicion (see sections 7.13 to 7.20). Unnecessary routing of funds through third party accounts means routing without clear economic (business) reasoning.
(…)		
		AML/CFT Systems in relation to ~~suspicious~~ transaction reporting
	9.7	A Relevant Person should implement appropriate AML/CFT Systems in order to fulfil its statutory reporting obligation, and properly manage and mitigate the risks associated with any customer or transaction involved in an STR or threshold transactions report (“TTR”). The AML/CFT Systems should include: (a) appointment of an MLRO (see Part 4); (b) implementing clear policies and procedures over internal reporting, reporting to the FIU, post- reporting risk mitigation and prevention of tipping-off; and (c) keeping proper records of internal reports and STRs.
	9.8	The Relevant Person should have measures in place to check, on an ongoing basis, that its AML/CFT Systems in relation to suspicious transaction reporting comply with relevant legal and regulatory requirements and operate effectively. The type and extent of the measures to be taken should be appropriate having regard to the risk of ML/TF as well as the nature and size of the business. The policies, procedures, systems and controls to monitor and detect transactions above defined thresholds, and submission of TTRs to the FIU should be performed in accordance with the National AML Law.
(…)		
		Record-keeping
(…)		
	9.30	A Relevant Person must establish and maintain a record of all STRs made to the FIU. The record should include details of

		the date of the STR, the person who made the STR, and information to allow the papers relevant to the STR to be located. This register may be combined with the register of internal reports, if considered appropriate. A Relevant Person must establish and maintain a record of all TTRs made to the FIU.

(…)

ANNEX 1

RISK INDICATORS FOR ASSESSING ML/TF RISKS

The following is a list of non-exhaustive illustrative risk indicators for business risk assessment and customer risk assessment. These examples of indicators associated with each risk factor mentioned in sections 3.8 and 3.20 may indicate higher or lower ML/TF risks as the case may be.

(…)		
Customer risk	2	Examples of customers that may present higher ML/TF risk include: (a) the business relationships established in unusual circumstances (e.g. a customer instructs a Relevant Person to set up a discretionary management agreement for an investment vehicle owned by the customer but requests the Relevant Person to buy and sell particular securities for the investment vehicle only according to the customer's instructions); (b) non-resident customers who have no discernible reasons for opening an account with Relevant Persons in the Republic of Kazakhstan (AIFC); (c) the use of legal persons or arrangements as personal asset-holding vehicles without any commercial or other valid reasons; (d) companies that have nominee shareholders or shares in bearer form; (e) customers that engage in, or derive wealth or revenues from, cash-intensive businesses; (f) the ownership structure of a company appears unusual or excessively complex having considered the nature of

		the company's business; (g) the customer or the family member or close associate of a customer is a PEP (including where a beneficial owner of a customer is a PEP); (h) customers that have been mentioned in negative news reports from credible media, particularly those related to predicate offences for ML/TF or financial crimes; (i) nature, scope and location of business activities generating the funds may be related to high risk activities or jurisdictions posing a higher risk; (j) customers that have sanction exposure; (k) where the origin of wealth (for high risk customers and PEPs) or ownership cannot be easily verified; and (l) a customer introduced by an overseas financial institution, affiliate or other investor, both of which are based in jurisdictions posing a higher risk;~~.~~ (m) the activity or transactions of the customer does not correspond the customer risk profile. Examples of customers that may be considered to carry lower ML/TF risk include: (a) specific types of customers that may be eligible for SDD as specified in section 5.59; (b) customers who are employment-based or with a regular source of income from a known legitimate source which supports the activity being undertaken; and (c) the reputation of the customer, e.g. a well-known, reputable private company, with a long history that is well documented by independent sources, including information regarding its ownership and control.

ANNEX 2

INDICATORS OF SUSPICIOUS TRANSACTIONS AND ACTIVITIES

The following is a list of non-exhaustive indicators of suspicious transactions and activities that, along with the FIU's list set out in its regulation, may help assess whether or not transactions and activities might give rise to grounds of ML/TF suspicion.

(…)		
Unusual activity for virtual currency (VC), virtual assets (VA), virtual asset service providers (VASPs)	9	**Indicators linked to operations** (a) Structuring transactions with D~~V~~A (transactions of exchange or transfer), carried out in a similar way to structuring transactions with cash, by breaking into small amounts or into amounts that do not exceed the thresholds established for mandatory registration of transactions or for reporting; (b) Making multiple high-value transactions or in short succession, such as within a 24-hour period; or in a staggered and regular pattern, with no further transactions recorded during a long period afterwards (which is particularly common in ransomware-related cases) or to a newly created or to a previously inactive account; (c) Transferring D~~V~~As immediately to multiple D~~V~~ASPs, especially to D~~V~~ASPs registered or operated in another jurisdiction where there is no relation to where the customer lives or conducts business; or o there is non-existent or weak AML/CFT regulation; (d) Depositing D~~V~~As at an exchange and then often immediately – (i) withdrawing the D~~V~~As without additional exchange activity to other D~~V~~As (which is an unnecessary step and incurs transaction fees); (i) converting the D~~V~~As to multiple types of D~~V~~As, again incurring additional transaction fees, but without logical business explanation (e.g. portfolio diversification); or (ii) withdrawing the D~~V~~As from a D~~V~~ASP immediately to a private wallet (this effectively turns the exchange/D~~V~~ASP into an ML mixer); (e) Accepting funds suspected as stolen or fraudulent – (i) depositing funds from D~~V~~A addresses that have been identified as holding stolen funds, or D~~V~~A addresses linked to the holders of stolen funds.
	9.1	**Indicators related to Transaction Patterns** *New user transactions* (a) Conducting a large initial deposit to open a new relationship with a D~~V~~ASP, while the amount funded is inconsistent with the customer profile; (b) Conducting a large initial deposit to open a new relationship with a D~~V~~ASP and funding the entire deposit the

		first day it is opened, and that the customer starts to trade the total amount or a large portion of the amount on that same day or the day after, or if the customer withdraws the whole amount the day after (as most VAs have a transactional limit for deposits, laundering in large amounts could also be done through over-the-counter-trading); (c) A new user attempts to trade the entire balance of VAs, or withdraws the D~~V~~As and attempts to send the entire balance off the platform; *Transactions relative to all users* (d) Transactions involving the use of multiple D~~V~~As, or multiple accounts, with no logical business explanation; (e) Frequent transfers in a certain period of time (e.g. a day, a week, a month, etc.) to the same D~~V~~A account – or by more than one person; or from the same IP address by one or more persons; or concerning large amounts; (f) Incoming transactions from many unrelated wallets in relatively small amounts (accumulation of funds) with subsequent transfer to another wallet or full exchange for fiat currency. (Such transactions by a number of related accumulating accounts may initially use D~~V~~As instead of fiat currency); (g) Conducting D~~V~~A-fiat currency exchange at a potential loss (e.g. when the value of D~~V~~A is fluctuating, or regardless of abnormally high commission fees as compared to industry standards, and especially when the transactions have no logical business explanation); (h) Converting a large amount of fiat currency into D~~V~~As, or a large amount of one type of D~~V~~A into other types of D~~V~~As, with no logical business explanation.
	9.2	**Indicators related to anonymity** (a) Transactions by a customer involving more than one type of D~~V~~A, despite additional transaction fees, and especially those VAs that provide higher anonymity, such as anonymity-enhanced cryptocurrency (AEC) or privacy coins; (b) Moving a D~~V~~A that operates on a public, transparent blockchain, such as Bitcoin, to a centralised exchange and then immediately trading it for an AEC or privacy coin; (c) Customers that operate as an unregistered/unlicensed D~~V~~ASP on peer-to-peer (P2P) exchange websites, particularly when there are concerns that the customers handle huge amount of D~~V~~A transfers on its customer's behalf, and charge higher fees to its customer than transmission services offered by other

		exchanges. Use of bank accounts to facilitate these P2P transactions; (d) Abnormal transactional activity (level and volume) of D~~V~~As cashed out at exchanges from P2P platform-associated wallets with no logical business explanation; (e) VAs transferred to or from wallets that show previous patterns of activity associated with the use of D~~V~~ASPs that operate mixing or tumbling services or P2P platforms; (f) Transactions making use of mixing and tumbling services, suggesting an intent to obscure the flow of illicit funds between known wallet addresses and darknet marketplaces; (g) Funds deposited or withdrawn from a D~~V~~A address or wallet with direct and indirect exposure links to known suspicious sources, including darknet marketplaces, mixing/tumbling services, questionable gambling sites, illegal activities (e.g. ransomware) and/or theft reports; (h) The use of decentralised/unhosted, hardware or paper wallets to transport D~~V~~As across borders; (i) Users entering the D~~V~~ASP platform having registered their Internet domain names through proxies or using domain name registrars (DNS) that suppress or redact the owners of the domain names; (j) Users entering the D~~V~~ASP platform using an IP address associated with a darknet or other similar software that allows anonymous communication, including encrypted emails and VPNs. Transactions between partners using various anonymous encrypted communication means (e.g. forums, chats, mobile applications, online games, etc.) instead of a D~~V~~ASP; (k) A large number of seemingly unrelated D~~V~~A wallets controlled from the same IP-address (or MAC-address), which may involve the use of shell wallets registered to different users to conceal their relation to each other; (l) Use of D~~V~~As whose design is not adequately documented, or that are linked to possible fraud or other tools aimed at implementing fraudulent schemes, such as Ponzi schemes; (m) Receiving funds from or sending funds to D~~V~~ASPs whose CDD or know your customer (KYC) processes are demonstrably weak or non-exist; (n) Using D~~V~~A ATMs/kiosks – (i) despite the higher transaction fees and including those commonly used by mules or scam victims; (ii) in high-risk locations where increased criminal activities occur.

9.3 **Indicators related to senders or recipients**

Irregularities observed during account creation

(a) Creating separate accounts under different names to circumvent restrictions on trading or withdrawal limits imposed by D~~V~~ASPs;

(b) Transactions initiated from non-trusted IP addresses, IP addresses from sanctioned jurisdictions, or IP addresses previously flagged as suspicious;

(c) Trying to open an account frequently within the same D~~V~~ASP from the same IP address;

(d) Regarding merchants/corporate users, their Internet domain registrations are in a different jurisdiction than their jurisdiction of establishment or in a jurisdiction with a weak process for domain registration;

Irregularities observed during CDD process

(e) Incomplete or insufficient KYC information, or a customer declines requests for KYC documents or inquiries regarding source of funds;

(f) Sender / recipient lacking knowledge or providing inaccurate information about the transaction, the source of funds, or the relationship with the counterparty;

(g) Customer has provided forged documents or has edited photographs and/or identification documents as part of the on-boarding process;

Customer Profile

(h) A customer provides identification or account credentials (e.g. a non-standard IP address, or flash cookies) shared by another account;

(i) Discrepancies arise between IP addresses associated with the customer’s profile and the IP addresses from which transactions are being initiated;

(j) A customer’s D~~V~~A address appears on public forums associated with illegal activity;

(k) A customer is known via publicly available information to law enforcement due to previous criminal association;

Profile of potential money mule or scam victims

		(l) Sender does not appear to be familiar with DA technology or online custodial wallet solutions. Such persons could be money mules recruited by professional money launderers, or scam victims turned mules who are deceived into transferring illicit proceeds without knowledge of their origins; (m) A customer significantly older than the average age of platform users opens an account and engages in large numbers of transactions, suggesting their potential role as a D~~V~~A money mule or a victim of elder financial exploitation; (n) A customer being a financially vulnerable person, who is often used by drug dealers to assist them in their trafficking business; (o) Customer purchases large amounts of D~~V~~A not substantiated by available wealth or consistent with his or her historical financial profile, which may indicate money laundering, a money mule, or a scam victim; *Other unusual behaviour* (p) A customer frequently changes his or her identification information, including email addresses, IP addresses, or financial information, which may also indicate account takeover against a customer; (q) A customer tries to enter into one or more D~~V~~ASPs from different IP addresses frequently over the course of a day; (r) Use of language in D~~V~~A message fields indicative of the transactions being conducted in support of illicit activity or in the purchase of illicit goods, such as drugs or stolen credit card information; (s) A customer repeatedly conducts transactions with a subset of individuals at significant profit or loss. (This could indicate potential account takeover and attempted extraction of victim balances via trade, or ML scheme to obfuscate funds flow with a D~~V~~ASP infrastructure).
	9.4	**Indicators related to the source of wealth or funds** (a) Transacting with D~~V~~A addresses or bank cards that are connected to known fraud, extortion, or ransomware schemes, sanctioned addresses, darknet marketplaces, or other illicit websites; (b) VA transactions originating from or destined to online gambling services; (c) The use of one or multiple credit and/or debit cards that are linked to a D~~V~~A wallet to withdraw large amounts of fiat currency (crypto-to-plastic), or funds for purchasing D~~V~~As are sourced from cash deposits into credit

		cards; (d) Deposits into an account or a D~~V~~A address are significantly higher than ordinary with an unknown source of funds, followed by conversion to fiat currency, which may indicate theft of funds; (e) Lack of transparency or insufficient information on the origin and owners of the funds, such as those involving the use of shell companies or those funds placed in an Initial Coin Offering (ICO) where personal data of investors may not be available or incoming transactions from online payments system through credit/pre-paid cards followed by instant withdrawal; (f) A customer's funds which are sourced directly from third-party mixing services or wallet tumblers; (g) Bulk of a customer's source of wealth is derived from investments in D~~V~~As, ICOs, or fraudulent ICOs, etc; (h) A customer's source of wealth is disproportionately drawn from D~~V~~As originating from other D~~V~~ASPs that lack AML/CFT controls.
	9.5	**Indicators related to geographical risks** (a) 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; (b) Customer utilises a D~~V~~A exchange or foreign-located MVTS in a high-risk jurisdiction lacking, or known to have inadequate, AML/CFT regulations for VA entities, including inadequate CDD or KYC measures; (c) Customer sends funds to D~~V~~ASPs operating in jurisdictions that have no D~~V~~A regulation, or have not implemented AML/CFT controls; (d) Customer sets up offices in or moves offices to jurisdictions that have no regulation or have not implemented regulations governing D~~V~~As, or sets up new offices in jurisdictions where there is no clear business rationale to do so.

(…)

Annex 7

INDEPENDENT AML AUDIT

(…)		
	2.	**Preparation for the AML audit**
	2.1	Like any other process, the audit should begin with proper preparation. To ensure an efficient audit, the company should evaluate its own AML/CTF programs over time, as this will be the first thing the auditor checks and assesses. Here are some questions to help focus on the relevant areas for preparation: ▪ Are the Business Risk Assessment and AML Policies and Internal Control Rules up to date? ▪ How the real procedures and controls are correlated with those outlined in Company's AML/CTF Programmes? ▪ When the last AML/CTF training took place and are the employees, including senior management, up to date with their AML/CTF training? ▪ Has the relevant function been doing Customer Due Diligence and Enhanced Due Diligence? ▪ Have the Customer's dossiers and Customer's AML/CTF profiles been updated? ▪ Has the relevant function undertaken transaction monitoring? ▪ Has the relevant function fulfilled the reporting requirements? ▪ Has the record-keeping been properly organised? ▪ Has the senior management and the MLRO been keeping frequent (regular) dialogue?

(…)